

One by one the guests arrive
 The guests are coming through
 And “Welcome, welcome” cries a voice
 “Let all my guests come in!”¹.

To S. J. Patterson, at his 60 - th birthday

SNOQIT I: GROWTH OF Λ -MODULES AND KUMMER THEORY

PREDA MIHĂILESCU

ABSTRACT. Let $A = \varprojlim_n$ be the projective limit of the p -parts of the class groups in some \mathbb{Z}_p -cyclotomic extension. The main purpose of this paper is to investigate the transition $\Lambda a_n \rightarrow \Lambda a_{n+1}$ for some special $a = (a_n)_{n \in \mathbb{N}} \in A$, of infinite order. Using an analysis of the $\mathbb{F}_p[T]$ -modules $\mathcal{A}_n/p\mathcal{A}_n$ and $\mathcal{A}_n[p]$ we deduce some restrictive conditions on the structure and rank of these modules. Our model can be applied also to a broader variety of cyclic p -extensions and associated modules. In particular, it applies to certain cases of subfields of Hilbert or Takagi class fields, i.e. finite cyclic extensions.

As a consequence of this taxonomy (The term of *taxonomic* research was coined by Samuel Patterson; it very well applies to this work and is part of the dedication at the occasion of his 60-th birthday) we can give a proof in CM fields of the conjecture of Gross concerning the non vanishing of the p -adic regulator of p -units.

CONTENTS

1. Introduction	2
1.1. Notations	5

¹Leonard Cohen: *The Guests*.

Date: Version 2.10 January 26, 2013.

The first results of this paper were developed before the year 2008, while the author was sponsored by a grant of the Volkswagen Foundation. Some of the central questions were first considered during the month of February 2010, spent as a guest professor in Caen, at the invitation of Bruno Anglès: these led also to the more recent developments.

SNOQIT=“SEMINAR NOTES ON OPEN QUESTIONS IN IWASAWA THEORY” REFERS TO A SEMINAR HELD TOGETHER WITH J.S.PATTERSON IN 2007/08.

1.2.	List of symbols	5
1.3.	Ramification and its applications	6
1.4.	Sketch of the proof	7
2.	Growth of Λ -modules	9
2.1.	The notion of conic modules and elements	9
2.2.	Auxiliary identities and lemmata	10
2.3.	Stabilization	12
2.4.	The case of increasing ranks	16
2.5.	Transition modules and socles	18
2.6.	Case distinctions for the rank growth	27
3.	Transitions and the critical section	29
3.1.	Proof of Theorem 1	31
3.2.	Some examples	31
4.	The ramification module	34
4.1.	Kummer theory, radicals and the order reversal	35
4.2.	Units and the radical of Ω	37
4.3.	Construction of auxiliary extension and order reversal	39
4.4.	The contribution of class field theory	41
4.5.	Proof of Theorems 3 and 1	44
5.	Conclusions	45
	References	47

1. INTRODUCTION

Let p be an odd prime and $\mathbb{K} \supset \mathbb{Q}[\zeta]$ be a galois extension containing the p -th roots of unity, while $(\mathbb{K}_n)_{n \in \mathbb{N}}$ are the intermediate fields of its cyclotomic \mathbb{Z}_p -extension \mathbb{K}_∞ . Let $A_n = (\mathcal{C}(\mathbb{K}_n))_p$ be the p -parts of the ideal class groups of \mathbb{K}_n and $\mathbf{A} = \varprojlim_n A_n$ be their projective limit. The subgroups $\mathbf{B}_n \subset A_n$ are generated by the classes containing ramified primes above p and we let

$$(1) \quad \begin{aligned} A'_n &= A_n / \mathbf{B}_n, \\ \mathbf{B} &= \varprojlim_n \mathbf{B}_n, \quad \mathbf{A}' = \mathbf{A} / \mathbf{B}. \end{aligned}$$

We denote as usual the galois group $\Gamma = \text{Gal}(\mathbb{K}_\infty / \mathbb{K})$ and $\Lambda = \mathbb{Z}_p[\Gamma] \cong \mathbb{Z}_p[[\tau]] \cong \mathbb{Z}_p[[T]]$, where $\tau \in \Gamma$ is a topological generator and $T = \tau - 1$; we let

$$\omega_n = (T + 1)^{p^{n-1}} - 1 \in \Lambda, \quad \nu_{n+1,n} = \omega_{n+1} / \omega_n \in \Lambda.$$

If X is a finite abelian group, we denote by X_p its p -Sylow group. The exponent of X_p is the smallest power of p that annihilates X_p ; the

subexponent

$$\text{sexp}(X_p) = \min\{ \text{ord}(x) : x \in X_p \setminus X_p^p \}.$$

Fukuda proves in [8] (see also Lemma 4 below) that if $\mu(\mathbb{K}) = 0$, then there for the least $n_0 \geq 0$ such that $p\text{-rk}(A_{n_0+1}) = p\text{-rk}(A_{n_0})$ we also have $p\text{-rk}(\mathbf{A}) = \text{prk}(A_{n_0})$: the p -rank of A_n becomes stationary after the first occurrence of a stationary rank. It is a general property of finitely generated Λ -modules of finite p -rank, that their p -rank must become stationary after some fixed level – the additional fact that this already happens after the first rank stabilization is a consequence of an early theorem of Iwasawa (see Theorem 2 below) which relates the Λ -module \mathbf{A} to class field theory. The theorem has a class field theoretical proof and one can show that the properties it reveals are not shared by arbitrary finitely generated Λ -modules.

The purpose of this paper is to pursue Fukuda's observation at the level of individual cyclic Λ -modules and also investigate the *prestable* segment of these modules. We do this under some simplifying conditions and focus on specific cyclic Λ -modules defined as follows:

Definition 1. Let \mathbb{K} be a CM field and $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^-$ have infinite order. We say that a is conic¹ if the following conditions are fulfilled:

1. There is a Λ -submodule $\mathbf{C} \subset \mathbf{A}^-$ such that

$$\mathbf{A}^- = \mathbf{C} \oplus \Lambda a.$$

We say in this case that Λa is Λ -complementable.

2. Let $c = (c_n)_{n \in \mathbb{N}} \in \Lambda a$. If $c_n = 1$ for some $n > 0$, then $c \in \omega_n(\Lambda a)$.
3. If $b \in \mathbf{A}^-$ and there is a power $q = p^k$ with $b^q \in \Lambda a$, then $b \in \Lambda a$.
4. If $f_a(T) \in \mathbb{Z}_p[T]$ is the exact annihilator of Λa , then $(f_a(T), \omega_n(T)) = 1$ for all $n > 0$.

The above definition is slightly redundant, containing all the properties that we shall require. See also §2.1 for a more detailed discussion of the definition.

The first purpose of this paper is to prove the following theorem.

Theorem 1. Let p be an odd prime, \mathbb{K} be a galois CM extension containing a p -th root of units and let \mathbb{K}_n, A_n and \mathbf{A} be defined like above. Let $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^- \setminus (\mathbf{A}^-)^p$ be conic, $q = \text{ord}(a_1)$ and let $f_a(T)$

¹One can easily provide examples of non conic elements, by considering \mathbb{K}_∞ as a \mathbb{Z}_p -extension of \mathbb{K}_n for some $n > 1$. It is an interesting question to find some conditions related only to the field \mathbb{K} , which assure the existence of conic elements.

be the exact annihilator polynomial of a . If $q = p$, then $f_a(T)$ is an Eisenstein polynomial. Otherwise, if n_0 is the least integer with $p\text{-rk}(\mathcal{A}_{n_0}) = p\text{-rk}(\mathcal{A}_{n_0+1})$ then either $n_0 \leq 3$ and the rank is bounded by

$$(2) \quad v_p(a_1) > 1 \quad \Rightarrow \quad p\text{-rk}(\Lambda a) < p(p-1),$$

or $n_0 > 3$ and $\text{sexp}(\mathcal{A}_{n_0-1}) = \exp(\mathcal{A}_{n_0-1})$. Moreover \mathcal{A}_{n_0} has an annihilator polynomial

$$f_{n_0}(T) = T^\lambda - qw(T), \quad \lambda = p\text{-rk}(\mathcal{A}), \quad w(T) \in (\mathbb{Z}_p[T])^\times,$$

and $f_a(T) - f_{n_0}(T) \in a_{n_0}^\top = \{x \in \mathbb{Z}_p[T] : a_{n_0}^x = 1\}$.

The theorem is obtained by a tedious algebraic analysis of the rank growth in the *transitions* $\mathcal{A}_n \hookrightarrow \mathcal{A}_{n+1}$.

A class of examples of conic modules is encountered for quadratic ground fields \mathbb{K} , such that the p -part $A_1(\mathbb{K})$ of the class group is \mathbb{Z}_p -cyclic. We shall give in section 3.2 a series of such examples, drawn from the computations of Ernvall and Metsänkilä in [6]. A further series of applications concern the structure of the components $e_{p-2k}\mathbf{A}$ of the class group of p -cyclotomic extensions, when the Bernoulli number $B_{2k} \equiv 0 \pmod{p}$. If the conjecture of Kummer - Vandiver or the cyclicity conjecture holds for this component, then the respective modules are conic.

The question about the detailed structure of annihilator polynomials in Iwasawa extensions is a difficult one and it has been investigated in a series of papers in the literature. For small, e.g. quadratic fields, a probabilistic approach yields already satisfactory results. In this respect, the Cohen-Lenstra [4] and Cohen-Martinet [5] heuristics have imposed themselves, being confirmed by a large amount of empirical results; see also Bhargava's use of these heuristics in [2] for recent developments.

At the other end, for instance in p -cyclotomic fields, computations only revealed linear annihilator polynomials. In spite of the improved resources of modern computers, it is probably still infeasible to pursue intensive numeric investigations for larger base fields. In this respect, we understand the present paper as a proposal for a new, intermediate approach between empirical computations and general proofs: *empirical case distinctions* leading to some structural evidence. In this sense, the conditions on conic elements are chosen such that some structural results can be achieved with feasible effort. The results indicate that for large base fields, the repartitions of exact annihilators of elements of \mathbf{A}^- can be expected to be quite structured and far from uniform repartition within all possible distinguished polynomials.

1.1. Notations. We shall fix some notations. The field \mathbb{K} is assumed to be a CM galois extension of \mathbb{Q} with group Δ , containing a p -th root of unity ζ but no p^2 -th roots of unity. We let $(\zeta_{p^n})_{n \in \mathbb{N}}$ be a norm coherent sequence of p^n -th roots of unity, so $\mathbb{K}_n = \mathbb{K}[\zeta_{p^n}]$. Thus we shall number the intermediate extensions of \mathbb{K}_∞ by $\mathbb{K}_1 = \mathbb{K}, \mathbb{K}_n = \mathbb{K}[\zeta_{p^n}]$. We have uniformly that \mathbb{K}_n contains the p^n -th but not the p^{n+1} -th roots of unity. In our numbering, ω_n annihilates \mathbb{K}_n^\times and all the groups related to \mathbb{K}_n ($A_n, \mathcal{O}(\mathbb{K}_n)$, etc.)

Let $A = \mathcal{C}(\mathbb{K})_p$, the p -Sylow subgroup of the class group $\mathcal{C}(\mathbb{K})$. The p -parts of the class groups of \mathbb{K}_n are denoted by A_n and they form a projective sequence with respect to the norms $N_{m,n} := \mathbf{N}_{\mathbb{K}_m/\mathbb{K}_n}, m > n > 0$, which are assumed to be surjective. The projective limit is denoted by $\mathbf{A} = \varprojlim_n A_n$. The submodule $\mathbf{B} \subset \mathbf{A}$ is defined by (1) and $\mathbf{A}' = \mathbf{A}/\mathbf{B}$. At finite levels $A'_n = A_n/\mathbf{B}_n$ is isomorphic to the ideal class group of the ring of the p -units in \mathbb{K}_n . The maximal p -abelian unramified extension of \mathbb{K}_n is \mathbb{H}_n and $\mathbb{H}'_n \subset \mathbb{H}_n$ is the maximal subfield that splits all the primes above p . Then $\text{Gal}(\mathbb{H}'_n/\mathbb{K}_n) \cong A'_n$ (e.g. [11], §3. - 4.).

If the coherent sequence $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^-$ is a conic element, then $p\text{-rk}(\Lambda a) < \infty$. We write $\mathcal{A} = \Lambda a$ and $\mathcal{A}_n = \Lambda a_n$: the finite groups \mathcal{A}_n form a projective sequence of Λ -modules with respect to the norms. The exact annihilator polynomial of \mathcal{A} is denoted by $f_a(T) \in \mathbb{Z}_p[T]$.

If $f \in \mathbb{Z}_p[T]$ is some distinguished polynomial that divides the characteristic polynomial of \mathbf{A} , we let $\mathbf{A}(f) = \cup_n \mathbf{A}[f^n]$ be the union of all power f -torsions in \mathbf{A} . Since \mathbf{A} is finitely generated, this is the maximal submodule annihilated by some power of f . If $B \subset \mathbf{A}(f)$ is some Λ -module, then we let $k = \text{ord}_f(B)$ be the least integer such that $f^k B = 0$.

1.2. List of symbols. We give here a list of the notations introduced below in connection with Iwasawa theory

p	A rational prime,
ζ_{p^n}	Primitive p^n -th roots of unity with $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for all $n > 0$.,
μ_{p^n}	$\{\zeta_{p^n}^k, k \in \mathbb{N}\}$,
\mathbb{K}	A galois CM extension of \mathbb{Q} containing the p -th roots of unity,
$\mathbb{K}_\infty, \mathbb{K}_n$	The cyclotomic \mathbb{Z}_p -extension of \mathbb{K} , and intermediate fields,
Δ	$\text{Gal}(\mathbb{K}/\mathbb{Q})$,
$A(\mathbf{K})$	= p -part of the ideal class group of the field \mathbf{K} ,
s	The number of primes above p in \mathbb{K} ,
Γ	$\text{Gal}(\mathbb{K}_\infty/\mathbb{K}) = \mathbb{Z}_p\tau$, τ a topological generator of Γ
T	= $\tau - 1$,
$*$	Iwasawa's involution on Λ induced by $T^* = (p - T)/(T + 1)$,

Λ	$\mathbb{Z}_p[[T]], \quad \Lambda_n = \Lambda/(\omega_n \Lambda),$
ω_n	$(T+1)^{p^{n-1}} - 1, \quad (\mathbb{K}_n^\times)^{\omega_n} = \{1\},$
$A'_n = A'(\mathbb{K}_n)$	The p - part of the ideal class group of the p - integers of \mathbb{K}_n ,
A'	$= \varprojlim A'_n,$
\mathbf{B}	$= \langle \{b = (b_n)_{n \in \mathbb{N}} \in A : b_n = [\wp_n], \wp_n \supset (p)\} \rangle_{\mathbb{Z}_p},$
\mathbb{H}_∞	The maximal p - abelian unramified extension of \mathbb{K}_∞ ,
$\mathbb{H}'_\infty \subset \mathbb{H}_\infty$	The maximal subextension of \mathbb{H}_∞ that splits the primes above p .

The following notations are specific for transitions:

(A, B)	$=$ A conic transition, A, B are finite $\mathbb{Z}_p[T]$ -modules,
G	$=$ $\langle \tau \rangle$, a cyclic p -group acting on the modules of the transition,
T	$=$ $\tau - 1$,
$S(X)$	$=$ $X[p]$, the p -torsion of the p group X , or its socle,
$R(X)$	$=$ $X/(pX)$, the “roof” of the p group X ,
N, ι	$=$ The norm and the lift associated to the transition (A, B) ,
K	$=$ $\text{Ker}(N : B \rightarrow A)$,
ω	$=$ Annihilator of A , such that $N = p + \omega N'$,
d	$=$ $\deg(\omega(T)); \quad \nu = \frac{(\omega+1)^p - 1}{\omega},$
$\nu\omega$	$=$ Annihilator of B ,
\mathcal{T}	$=$ $B/\iota(A)$, The transition module associated to (A, B) ,
s, s'	$=$ Generators of $S(A), S(B)$ as $\mathbb{F}_p[T]$ -modules,
a, b	$=$ Generators of A, B as $\mathbb{Z}_p[T]$ -modules,
r, r'	$=$ $p\text{-rk}(A), p\text{-rk}(B)$.

1.3. Ramification and its applications. Iwasawa’s Theorem 6 [11] plays a central role in our investigations. Let us recall the statement of this theorem in our context (see also [16], Lemma 13.14 and 13.15 and [13], Chapter 5, Theorem 4.2):

Theorem 2 (Iwasawa, Theorem 6 [11]). *Let \mathbb{K} be a number field and $P = \{\wp_i : i = 1, 2, \dots, s\}$ be the primes of \mathbb{K} above p and assume that they ramify completely in $\mathbb{K}_\infty/\mathbb{K}$. Let $\mathbb{H}_\infty/\mathbb{K}_\infty$ be the maximal p -abelian unramified extension of \mathbb{K}_∞ and $H = \text{Gal}(\mathbb{H}_\infty/\mathbb{K})$, while $I_i \subset H, i = 1, 2, \dots, s$ are the inertia groups of some primes of \mathbb{H}_∞ above \wp_i . Let $a_i \in \mathbf{A}$ be such that $\varphi(\sigma_i)I_1 = I_i$, for $i = 2, 3, \dots, s$.*

For every $n > 0$ there is a module $Y_n = \omega_n \mathbf{A} \cdot [a_2, \dots, a_s]_{\mathbb{Z}_p}$ such that $\mathbf{A}/Y_n \cong \mathbf{A}_n$.

Note that the context of the theorem is not restricted to CM extensions. In fact Iwasawa’s theorem applies also to non cyclotomic \mathbb{Z}_p -extensions, but we shall not consider such extensions in this paper.

The following Theorem settles the question about Y_1^- in CM extensions:

Theorem 3. *Let \mathbb{K} be a galois CM extension of \mathbb{Q} and \mathbf{A} be defined like above. Then $\mathbf{A}^-(T) = \mathbf{A}^-[T] = \mathbf{B}^-$.*

We prove the theorem in Chapter 4. Then we derive from Theorem 3 the following result:

Corollary 1. *Let \mathbb{K} be a CM s -field and \mathbf{B}_n, A'_n be defined by (1). Then $(\mathbf{A}')^-[T] = \{1\}$.*

This confirms a conjecture of Gross and Kuz'min stated by Federer and Gross in [7] in the context of p -adic regulators of p -units of number fields, and earlier by Kuz'min [12] in a class field oriented statement, which was shown by Federer and Gross to be equivalent to the non vanishing of p -adic regulators of p -units. We prove here the class field theoretic statement for the case of CM fields. The conjecture was known to be true for abelian extensions, due to previous work of Greenberg [9].

1.4. Sketch of the proof. We start with an overview of the proof. Our approach is based on the investigation of the growth of the ranks $r_n := p\text{-rk}(\mathcal{A}_n) \rightarrow p\text{-rk}(\mathcal{A}_{n+1})$; for this we use *transitions* $C_n := \mathcal{A}_{n-1}/\iota_{n,n+1}(\mathcal{A}_n)$, taking advantage of the fact that our assumptions assure that the ideal lift maps are injective for all n . Since we also assumed $p\text{-rk}(\mathcal{A}) < \infty$, it is an elementary fact that the ranks r_n must stabilize for sufficiently large n . Fukuda proved recently that this happens after the first n for which $r_n = r_{n+1}$. We call this value n_0 : the *stabilization index*, and focus upon the *critical section* $\mathcal{A}_n : n < n_0$. In this respect, the present work is inspired by Fukuda's result and extends it with the investigation of the critical section; this reveals useful criteria for stabilization, which make that the growth of conic Λ -modules is quite controlled: at the exception of some modules with *flat* critical section, which can grow in rank indefinitely, but have constant exponent p^k , the rank is bounded by $p(p-1)$.

The idea of our approach consists in modeling the *transitions* $(A, B) = (\mathcal{A}_n, \mathcal{A}_{n+1})$ by a set of dedicated properties that are derived from the properties of conic elements. The conic transitions are introduced in Definition 3 below. Conic transitions do not only well describe the critical section of conic Λ -modules, but they also apply to sequences A_1, A_2, \dots, A_n of more general finite modules on which a p -cyclic group $\langle \tau \rangle$ acts via the group ring $\mathbf{R} = \mathbb{Z}/(p^N \cdot \mathbb{Z})[\tau] = \mathbb{Z}_p[T], T = \tau - 1$, with $p^N A_n = 0$; the modules A, B are in particular assumed to be cyclic as \mathbf{R} -modules and they fulfill some additional properties with respect to norms and lifts. As a consequence, the same theory can be

applied for instance to sequences of class groups in cyclic p -extensions, ramified or unramified.

The ring \mathbf{R} is a local ring with maximal ideal (p, T) ; since this ideal is not principal, it is customary to use the Fitting ideals for the investigation of modules on which \mathbf{R} acts. Under the additional conditions of conicity however, the transitions (A, B) come equipped with a wealth of useful $\mathbb{F}_p[T]$ -modules. Since $\mathbb{F}_p[T]$ has a maximal ideal (T) , which is principal, this highly simplifies the investigation. The most important $\mathbb{F}_p[T]$ -modules related to a transition are the *socle*, $S(B) = B[p]$ and the *roof*, $R(B) = B/pB$. It is a fundamental, but not evident fact, that $S(B)$ is a cyclic $\mathbb{F}_p[T]$, and we prove this by induction in Lemma 8. With this, the transitions are caught between two pairs of cyclic $\mathbb{F}_p[T]$ -modules, and the relation between these modules induces obstructions on the growth types. These obstructions are revealed in a long sequence of tedious case distinctions, which develop in a natural way.

The relation between rank growth and norm coherence reveals in Corollary 2 the principal condition for termination of the rank growth: assuming that $p\text{-rk}(A_1) = 1$, this must happen as soon as $p\text{-rk}(A_n) < p^{n-1}$. This is a simple extension of Fukuda's results, giving a condition for growth termination, not only for rank stabilization. A further important module associated to the transition is the kernel of the norm, $K := \text{Ker}(N : B \rightarrow A)$. The structure of K is an axiom of conic transitions, which is proved to hold in the case of conic Λ -modules. The analysis of growth in conic transitions is completed in the Chapter 2.

In Chapter 3, the analysis of transitions can be easily adapted to conic Λ -modules, yielding an inductive proof of their structure, as described in Theorem 1. In the fourth chapter we prove the Theorem 3 and Corollary 1.

Except for the second Chapter, the material of this paper is quite simple and straight forward. In particular, the main proof included in Chapter 3 follows easily from the technical preparation in Chapter 2. Therefore the reader wishing to obtain first an overview of the main ideas may skip the second chapter in a first round and may even start with Chapter 4, in case her interest goes mainly in the direction of the proof of the conjectures included in that chapter.

The Lemmata 4, 5 are crucial for our approach to Kummer theory. They imply the existence of some index $n_0 \geq 0$ such that for all coherent sequences $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}$ of infinite order, there is a constant $z =$

$z(a) \in \mathbb{Z}$ such that:

$$(3) \quad \begin{aligned} p\text{-rk}(\mathcal{A}_n) &= p\text{-rk}(\mathcal{A}_{n_0}), \\ a_{n+1}^p &= \iota_{n,n+1}(a_n) \\ \text{ord}(a_n) &= p^{n+z}. \end{aligned}$$

2. GROWTH OF Λ -MODULES

We start with a discussion of the definition of conicity:

2.1. The notion of conic modules and elements. We have chosen in this paper a defensive set of properties for conic modules, in order to simplify our analysis of the growth of Λ -modules. We give here a brief discussion of these choices. The restriction to CM fields and submodules $\Lambda a \subset \mathbf{A}^-$ is a sufficient condition for ensuring that all lift maps $\iota_{n,n+1}$ are injective. One can prove in general that for a of infinite order, these maps are injective beyond a fixed stabilization index n_0 that will be introduced below. For $n < n_0$ the question remains still open, if it suffices to assume that $\text{ord}(a) = \infty$ in order to achieve injectivity at all levels. It is conceivable that the combination of the methods developed in this paper may achieve this goal, but the question allows no simple answer, so we defer it to latter investigations.

By assuming additionally that $(f_a(T), \omega_n(T)) = 1$, we obtain as a consequence of these assumptions, that for $x = (x_m)_{m \in \mathbb{N}}$ with $x_m = 1$, we have $x \in \omega_n \mathbf{A}$. In the same vein, if $x_m^{\omega_n} = 1$ for $m > n$, then $x_m \in \iota_{n,m}(\mathcal{A}_n)$. These two consequences are very practical and will be repeatedly applied below.

The fundamental requirement to conic elements $a \in \mathbf{A}$, is that the module Λa has a direct complement which is also a Λ -module. Conic modules exist – see for instance Corrolary 1 or the case of imaginary quadratic extensions \mathbb{K} with \mathbb{Z}_p cyclic $(\mathcal{C}(\mathbb{K}))_p$ and only one prime above p . The simplifying assumption allows to derive interesting properties of the growth of Λ -modules, that may be generalized to arbitrary modules.

This condition in fact implies the property 3. of the definition 1, a condition which we also call \mathbb{Z}_p -*coalescence closure* of Λa , meaning that Λa is equal to the smallest \mathbb{Z}_p -submodule of \mathbf{A} , which contains Λa and has a direct complement as a \mathbb{Z}_p -module. Certainly, given property 1 and using additive notation, $b = g(T)a + x, x \in \mathbf{B}, g \in \mathbb{Z}_p[T]$, and then $qb \in \Lambda a$ implies by property 1 that $qx = 0$, so b is twisted by a p -torsion element, which is inconsistent with the fact that \mathbf{A}^- was assumed \mathbb{Z}_p -torsion free. It is also an interesting question, whether the assumption of property 1 and $a_i \in T\mathbf{A}$ are sufficient to imply property 1.

2.2. Auxiliary identities and lemmata. We shall frequently use some identities in group rings, which are grouped below. For $n > 0$ we let $\mathbf{R}_n = \mathbb{Z}/(p^N \cdot \mathbb{Z})[T]/(\omega_n)$ for some large $N > 0$, satisfying $N > \exp(A_n)$. The ring \mathbf{R}_n is local with maximal ideal (ω_n) and we write \bar{T} for the image of T in this ring. Since $\bar{T}^{p^n} \in p\mathbf{R}_n$, it follows that $\bar{T}^{p^{n+N}} = 0$; thus $\bar{T} \in \mathbf{R}_n$ is nilpotent and \mathbf{R}_n is a principal ideal domain.

We also consider the group ring $\mathbf{R}'_n := \mathbb{Z}/(p^N \cdot \mathbb{Z})[\omega_n]/(\nu_{n+1,n})$, which is likewise a local principal ideal domain with maximal ideal generated by the nilpotent element ω_n . From the binomial development of $\nu_{n+1,n}$ we deduce the following fundamental identities in Λ

$$\begin{aligned}
 \nu_{n+1,n} &= \frac{(\omega_n + 1)^p - 1}{\omega_n} = \omega_n^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} / p \cdot \omega_n^{i-1} \\
 (4) \quad &= p(1 + O(\omega_n)) + \omega_n^{p-1} = \omega_n^{p-1} + pu(\omega_n), \\
 &u(\omega_n) = 1 + \frac{p-1}{2}\omega_n + \dots + \omega_n^{p-2} \in \Lambda^\times, \\
 \omega_n^p &= \omega_n \cdot (\nu_{n+1,n} - pu(\omega_n)) = \omega_{n+1} - p\omega_n u(\omega_n).
 \end{aligned}$$

The above identities are equivariant under the Iwasawa involution $*$: $\tau \mapsto (p+1)\tau^{-1}$. Note that we fixed the cyclotomic character $\chi(\tau) = p+1$. If $f(T) \in \Lambda$, we write $f^*(T) = f(T^*)$, the *reflected* image of $f(T)$. The reflected norms are $\nu_{n+1,n}^* = \omega_{n+1}^*/\omega_n^*$. From the definition of ω_n^* we have the following useful identity:

$$(5) \quad \omega_n + t\omega_n^* = p^{n-1}c, \quad t \in \Lambda_n^\times, c \in \mathbb{Z}_p^\times.$$

We shall investigate of the growth of the modules A_n for $n \rightarrow n+1$. Suppose now that A is a finite abelian p -group which is cyclic as an $\mathbb{Z}_p[T]$ -module, generated by $a \in A$. We say that a monic polynomial $f \in \mathbb{Z}_p[T]$ is a *minimal polynomial* for a , if f has minimal degree among all monic polynomials $g \in a^\top = \{x \in \mathbb{Z}_p[T] : xa = 0\} \subset \mathbb{Z}_p[T]$.

We note the following consequence of Weierstrass preparation:

Lemma 1. *Let $I = (g(T)) \subset \mathbb{Z}_p[T]$ be an ideal generated by a monic polynomial $g(T) \in \mathbb{Z}_p[T]$. If $n = \deg(g)$ is minimal amongst all the degrees of monic polynomials generating I , then $g(T) = T^n + ph(T)$, with $h(T) \in \mathbb{Z}_p[T]$ and $\deg(h) < n$.*

Proof. Let $g(T) = T^n + \sum_{i=0}^{n-1} c_i T^i$. Suppose that there is some $i < n$ such that $p \nmid c_i$. Then the Weierstrass Preparation Theorem ([16], Theorem 7.3) implies that $g(T)\mathbb{Z}_p[T] = g_2(T)\mathbb{Z}_p[T]$, for some polynomial with $\deg(g_2(T)) \leq n$, which contradicts the choice of g . Therefore $p \mid c_i$ for all $0 \leq i < n$, which completes the proof of the lemma. \square

Remark 1. *As a consequence, if A is a finite abelian group which is a Λ -cyclic module of p -rank n , then there is some polynomial $g(T) = T^r - ph(T)$ which annihilates A .*

We shall use the following simple application of Nakayama's Lemma:

Lemma 2. *Let X be a finite abelian p -group of p -rank r and $\mathcal{X} = \{x_1, x_2, \dots, x_r\} \subset X$ be a system with the property that the images $\bar{x}_i \in X/pX$ form a base of this \mathbb{F}_p -vector space. Then \mathcal{X} is a system of generators of X .*

Proof. This is a direct consequence of Nakayama's Lemma, [14], Chapter VI, §6, Lemma 6.3. \square

The following auxiliary lemma refers to elementary abelian p groups with group actions.

Lemma 3. *Let E be an additively written finite abelian² p -group of exponent p . Suppose there is a cyclic group $G = \langle \tau \rangle$ of order p acting on E , and let $T = \tau - 1$. Then E is an $\mathbb{F}_p[T]$ -module and E/TE is an \mathbb{F}_p -vector space. If $r = \dim_{\mathbb{F}_p}(E/TE)$, then every system $\mathcal{E} = \{e_1, e_2, \dots, e_r\} \subset E$ such that the images $\bar{e}_i \in E/(TE)$ form a base of the latter vector space, is a minimal system of generators of E as an $\mathbb{F}_p[T]$ -module. Moreover $E[T] \cong E/(TE)$ as \mathbb{F}_p -vector spaces and $E = \oplus_{i=1}^r \mathbb{F}_p[T]e_i$ is a direct sum of r cyclic $\mathbb{F}_p[T]$ -modules.*

Proof. The modules $E[T]$ and E/TE are by definition annihilated by T ; since $\mathbb{F}_p[T]/(T\mathbb{F}_p[T]) \cong \mathbb{F}_p$, they are finite dimensional \mathbb{F}_p -vector spaces. Let \mathcal{E} be defined like in the hypothesis. The ring $\mathbb{F}_p[T]$ is local with principal maximal ideal $T\mathbb{F}_p[T]$, and T is a nilpotent of the ring since $\tau^p = 1$ so we have the following identities in $\mathbb{F}_p[\tau] = \mathbb{F}_p[T]$: $0 = \tau^p - 1 = (T + 1)^p - 1 = T^p$. It follows from Nakayama's Lemma, that \mathcal{E} is a minimal system of generators. The map $T : E \rightarrow E$ is a nilpotent linear endomorphism of the \mathbb{F}_p -vector space E , so the structure theorem for Jordan normal forms of nilpotent maps implies that $E = \oplus_{i=1}^r \mathbb{F}_p[T]e_i$. One may also read this result by considering the exact sequence

$$0 \longrightarrow E[T] \longrightarrow E \longrightarrow E \longrightarrow E/(TE) \longrightarrow 0$$

in which the arrow $E \rightarrow E$ is the map $e \mapsto Te$. The diagram indicates that $E[T] \cong E/(TE)$, hence the claim. \square

In the situation of Lemma 3, we denote the common \mathbb{F}_p -dimension of $E[T]$ and E/TE by T -rank of E .

²These groups are sometimes denoted by *elementary abelian p -groups*, e.g. [16], §10.2.

2.3. Stabilization. We shall prove in this section the relations (3). First we introduce the following notations:

Definition 2. *given a finite abelian p -group X , we write $S(X) = X[p]$ for its p -torsion: we denote this torsion also by the socle of X . Moreover the factor $X/X^p = R(X)$ – the roof of X . Then $S(X)$ and $R(X)$ are \mathbb{F}_p -vector spaces and we have the classical definition of the p -rank given by $p\text{-rk}(X) = \text{rank}(S(X)) = \text{rank}(R(X))$, the last two ranks being dimensions of \mathbb{F}_p -vector spaces. We say that $x \in X$ is p -maximal, or simply maximal, if $x \notin X^p$.*

Suppose there is a cyclic p -group $G = \tau$ acting on X , such that X is a cyclic $\mathbb{Z}_p[T]$ -module with generator $x \in X$, where $T = \tau - 1$. Suppose additionally that $S(X)$ is also a cyclic $\mathbb{F}_p[T]$ -module. Let $s := (\text{ord}(x)/p)x \in S(X)$. Then we say that S is straight if s generates $S(X)$ as an $\mathbb{F}_p[T]$ -module; otherwise, $S(X)$ is folded.

The next lemma is a special case of Fukuda's Theorem 1 in [8]:

Lemma 4 (Fukuda). *Let \mathbb{K} be a CM field and A_n, \mathbf{A} be defined like above. Suppose that $\mu(\mathbf{A}^-) = 0$ and there is an $n_0 > 0$, such that $p\text{-rk}(A_{n_0}^-) = p\text{-rk}(A_{n_0+1}^-)$. Then $p\text{-rk}(A_n^-) = p\text{-rk}(A_{n_0}^-) = \lambda^-$ for all $n > n_0$.*

Remark 2. *The above application of Fukuda's Theorem requires $\mu = 0$; it is known that in this case the p -rank of A_n must stabilize, but here it is shown that it must stabilize after the first time this rank stops growing from A_n to A_{n+1} . We have restricted the result to the minus part which is of interest in our context. Note that the condition $\mu = 0$ can be easily eliminated, by considering the module $(\mathbf{A}^-)^{p^m}$ for some $m > \mu$.*

The following elementary, technical lemma will allow us to draw additional information from Lemma 4.

Lemma 5. *Let A and B be finitely generated abelian p -groups denoted additively, and let $N : B \rightarrow A$, $\iota : A \rightarrow B$ two \mathbb{Z}_p -linear maps such that:*

1. *N is surjective and ι is injective³;*
2. *The p -ranks of A and B are both equal to r and $|B|/|A| = p^r$.*
3. *$N(\iota(a)) = pa, \forall a \in A$ and ι is rank preserving, so $p\text{-rk}(\iota(A)) = p\text{-rk}(A)$;*

³The same results can be proved if the injectivity assumption is replaced by the assumption that $\text{sexp}(A) > p$ – injectivity then follows. In our context we injectivity is however part of the premises, so we give here the proof of the simpler variant of the lemma

Then $\iota(A) = pB$ and $\text{ord}(x) = p \cdot \text{ord}(Nx)$ for all $x \in B$.

Proof. The condition 3. is certainly fulfilled when ι is injective, as we did, but it also follows from $\text{sexp}(A) > p$, even for lift maps that are not injective. We start by noting that for any finite abelian p -group A of p -rank r and any pair $\alpha_i, \beta_i; i = 1, 2, \dots, r$ of minimal systems of generators there is a matrix $E \in \text{Mat}(r, \mathbb{Z}_p)$ which is invertible over \mathbb{Z}_p , such that

$$(6) \quad \vec{\beta} = E\vec{\alpha}.$$

This can be verified directly by extending the map $\alpha_i \mapsto \beta_i$ linearly to A and, since $(\beta_i)_{i=1}^r$ is also a minimal system of generators, deducing that the map is invertible, thus regular. It represents a unimodular change of base in the vector space $A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The maps ι and N induce maps

$$\bar{\iota} : A/pA \rightarrow B/pB, \quad \bar{N} : B/pB \rightarrow A/pA.$$

From 1, we see \bar{N} is surjective and since, by 2., it is a map between finite sets of the same cardinality, it is actually an isomorphism. But 3. implies that $\bar{N} \circ \bar{\iota} : A/pA \rightarrow A/pA$ is the trivial map and since \bar{N} is an isomorphism, $\bar{\iota}$ must be the trivial map, hence $\iota(A) \subset pB$.

Since ι is injective, it is rank preserving, i.e. $p\text{-rk}(A) = p\text{-rk}(\iota(A))$. Let $b_i, i = 1, 2, \dots, r$ be a minimal set of generators of B : thus the images \bar{b}_i of b_i in B/pB form an \mathbb{F}_p -base of this algebra. Let $a_i = N(b_i)$; since $p\text{-rk}(B/pB) = p\text{-rk}(A/pA)$, the set $(a_i)_i$ also forms a minimal set of generators for A . We claim that $|B/\iota(A)| = p^r$.

Pending the proof of this equality, we show that $\iota(A) = pB$. Indeed, we have the equality of p -ranks:

$$|B/pB| = |A/pA| = |B/\iota(A)| = p^r,$$

implying that $|pB| = |\iota(A)|$; since $\iota(A) \subset pB$ and the p -ranks are equal, the two groups are equal, which is the first claim. The second claim will be proved after showing that $|B/\iota(A)| = p^r$.

Let $S(X)$ denote the socle of the finite abelian p -group X . There is the obvious inclusion $S(\iota(A)) \subset S(B) \subset B$ and since ι is rank preserving, $p\text{-rk}(A) = p\text{-rk}(S(A)) = p\text{-rk}(B) = p\text{-rk}(S(B)) = p\text{-rk}(S(\iota(A)))$, thus $S(B) = S(\iota(A))$. Let $(a_i)_{i=1}^r$ be a minimal set of generators for A and $a'_i = \iota(a_i) \in B, i = 1, 2, \dots, r$; the $(a'_i)_{i=1}^r$ form a minimal set of generators for $\iota(A) \subset B$. We choose in B two systems of generators in relation to a'_i and the matrix E will map these systems according to (6).

First, let $b_i \in B$ be such that $p^{e_i}b_i = a'_i$ and $e_i > 0$ is maximal among all possible choices of b_i . From the equality of socles and p -ranks, one

verifies that the set $(b_i)_{i=1}^r$ spans B as a \mathbb{Z}_p -module; moreover, $\iota(A) \subset pB$ implies $e_i \geq 1$. On the other hand, the norm being surjective, there is a minimal set of generators $b'_i \in B$, $i = 1, 2, \dots, r$ such that $N(b'_i) = a_i$. Since b_i, b'_i span the same finite \mathbb{Z}_p -module B , (6) in which $\vec{\alpha} = \vec{b}$ and $\vec{\beta} = \vec{b}'$ defines a matrix with $\vec{b} = E \cdot \vec{b}'$. On the other hand,

$$\iota(\vec{a}) = \vec{a}' = \mathbf{Diag}(p^{e_i})\vec{b} = \mathbf{Diag}(p^{e_i})E \cdot \vec{b}',$$

The linear map $N : B \rightarrow A$ acts component-wise on vectors $\vec{x} \in B^r$. Therefore,

$$\begin{aligned} N\vec{b} &= N\vec{b}_i = N(E\vec{b}') = N\left(\left(\prod_j b'_j \sum_j e_{i,j}\right)_{i=1}^r\right) \\ &= \left(\prod_j (Nb'_j)^{\sum_j e_{i,j}}\right)_{i=1}^r = \left(\prod_j (a_j)^{\sum_j e_{i,j}}\right)_{i=1}^r \\ &= E(\vec{a}). \end{aligned}$$

Using the fact that the subexponent is not p , we obtain thus two expressions for $N\vec{a}'$ as follows:

$$\begin{aligned} N\vec{a}' &= p\vec{a} = pI \cdot \vec{a} \\ &= N\left(\mathbf{Diag}(p^{e_i})\vec{b}\right) = \mathbf{Diag}(p^{e_i}) \cdot N(\vec{b}) = \mathbf{Diag}(p^{e_i}) \cdot E\vec{a}, \quad \text{so} \\ \vec{a} &= \mathbf{Diag}(p^{e_i-1}) \cdot E\vec{a} \end{aligned}$$

The a_j form a minimal system of generators and E is regular over \mathbb{Z}_p ; therefore $\vec{\alpha} := (\alpha_j)_{j=1}^r = E\vec{a}$ is also minimal system of generators of A and the last identity above becomes

$$\vec{a} = \mathbf{Diag}(p^{e_i-1}) \cdot \vec{\alpha}.$$

If $e_i > 1$ for some $i \leq r$, then the right hand side is not a generating system of A while the left side is: it follows that $e_i = 1$ for all i . Therefore $|B/\iota(A)| = p^R$ and we have shown above that this implies the injectivity of ι .

Finally, let $x \in B$ and $q = \text{ord}(Nx) \geq p$. Then $qN(x) = 1 = N(qx)$, and since $qx \in \iota(A)$, it follows that $N(qx) = pqx = 1$ and thus pq annihilates x . Conversely, if $\text{ord}(x) = pq$, then $pqx = 1 = N(qx) = qN(x)$, and $\text{ord}(Nx) = q$. Thus $\text{ord}(x) = p \cdot \text{ord}(Nx)$ for all $x \in B$ with $\text{ord}(x) > p$. If $\text{ord}(x) = p$, then $x \in S(B) = S(\iota(A) \subset \iota(A))$ and $Nx = px = 1$, so the last claim holds in general. \square

One may identify the modules A, B in the lemma with subsequent levels A_n^- , thus obtaining:

Proposition 1. *Let \mathbb{K} be a CM field, let $\mathbf{A}^- = \varprojlim_n A_n^-$ and assume that $\mu(\mathbf{A}) = 0$. Let $n_0 \in \mathbb{N}$ be the bound proved in Lemma 4, such that for all $n \geq n_0$ and for all submodules $B \subset \mathbf{A}^-$ we have $p\text{-rk}(B_n) = \mathbb{Z}_p\text{-rk}(B) = \lambda(B)$. Then the following hold:*

$$(7) \quad \begin{aligned} px &= \iota(N_{n+1,n}(x)), & \iota(A_n^-) &= pA_{n+1}^-, \\ \omega_n x &\in \iota_{n,n+1}(A_n^-[p]) \end{aligned}$$

In particular, for $n > n_0$

$$(8) \quad \nu_{n+1,n}(a_{n+1}) = pa_{n+1} = \iota_{n,n+1}(a_n).$$

Proof. We let $n > n_0$. Since \mathbf{A}^- is \mathbb{Z}_p -torsion free, we may also assume that $\text{sexp}(A_n^-) > p$. We use the notations from Lemma 5 and let $\iota = \iota_{n,n+1}$, $N = N_{n+1,n}$ and $N' = \nu_{n+1,n}$.

For proving (8), thus $px = \iota(N(x)) = N'(x)$, we consider the development $t := \omega_n = (T+1)^{p^n} - 1$ and

$$N' = p + t \cdot v = p + t \left(\binom{p}{2} + tw \right), \quad v, w \in \mathbb{Z}[t],$$

as follows from the binomial development of $N' = \frac{(t+1)^p - 1}{t}$. By definition, t annihilates A_n^- and a fortiori $\iota(A_n^-) \subset A_{n+1}^-$; therefore, for arbitrary $x \in A_{n+1}^-$ we have $(pt)x = t(px) = t\iota(x_1) = 0$, where the existence of x_1 with $px = \iota(x_1)$, $x_1 \in A_n^-$ follows from Lemma 5. Since ι is injective and thus rank preserving, we deduce that $tx \in A_{n+1}^-[p] = \iota(A_n^-[p])$, which is the first claim in (7). Then

$$t^2x = t \cdot (tx) = tx_2 = 0, \quad \text{since } x_2 = tx \in \iota(A_n^-).$$

Using $t^2x = ptx = 0$, the above development for N' plainly yields $N'x = px$, as claimed. Injectivity of the lift map then leads to (7). Indeed, for $a = (a_n)_{n \in \mathbb{N}}$ and $n > n_0$ we have

$$\begin{aligned} \text{ord}(a_n) &= \text{ord}(\iota_{n+1,n}(a_n)) = \text{ord}(\iota_{n+1,n} \circ N_{n+1,n}(a_{n+1})) \\ &= \text{ord}(\nu_{n+1,n}a_{n+1}) = \text{ord}(pa_{n+1}) = \text{ord}(a_{n+1})/p. \end{aligned}$$

This completes the proof. \square

Remark 3. *The restriction to the minus part \mathbf{A}^- is perfectly compatible with the context of this paper. However, we note that Lemma 5 holds as soon as $\text{sexp}(A) > p$. As a consequence, all the facts in Proposition 1 hold true for arbitrary cyclic modules Λa with $\text{ord}(a) = \infty$. The proof being algebraic, it is not even necessary to assume that \mathbb{K}_∞ is the cyclotomic Λ -extension of \mathbb{K} , it may be any \mathbb{Z}_p -extension and $\mathbf{A} = \varprojlim_n A_n$ is defined with respect to the p -Sylow groups of the class groups in the*

intermediate levels of \mathbb{K}_∞ . The field \mathbb{K} does not need to be CM either. The Proposition 1 is suited for applications in Kummer theory, and we shall see some in the Chapter 4. This remark shows that the applications reach beyond the frame imposed in this paper.

As a consequence we have the following elegant description of the growth of orders of elements in A_n^- :

Lemma 6. *Let \mathbb{K} be a CM field and A_n, \mathbf{A} be defined as above, with $\mu(\mathbf{A}) = 0$. Then there exists an $n_0 > 0$ which only depends on \mathbb{K} , such that:*

1. $p\text{-rk}(A_n^-) = p\text{-rk}(A_{n_0}^-) = \lambda^-$ for $n \geq n_0$,
2. For all $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^-$ there is a $z = z(a) \in \mathbb{Z}$ such that, for all $n \geq n_0$ (3) holds.

Proof. The existence of n_0 follows from Lemma 4 and relation (7) implies that $\text{ord}(a_n) = p^{n-n_0} \text{ord}(a_{n_0})$ for all $n \geq n_0$, hence the definition of z . This proves point 2 and (3). \square

The above identities show that the structure of \mathcal{A} is completely described by \mathcal{A}_{n_0} : both the rank and the annihilator $f_a(T)$ of \mathcal{A} are equal to rank and annihilator of \mathcal{A}_{n_0} . Although \mathcal{A}_{n_0} is a finite module and thus its annihilator ideal is not necessarily principal, since it also contains ω_{n_0+1} and p^{n+z} , the polynomial $f_a(T)$ is a distinguished polynomial of least degree, contained in this ideal. Its coefficients may be normed by choosing minimal representatives modulo p^{n+z} . It appears that the full information about \mathcal{A} is contained in the *critical section* $\{\mathcal{A}_n : n \leq n_0\}$.

2.4. The case of increasing ranks. In this section we shall give some generic results similar to Lemma 5, for the case when the groups A and B have distinct ranks. Additionally, we assume that the groups A and B are endowed with a common group action which is reminiscent from the action of Λ on the groups \mathcal{A}_n of interest.

The assumptions about the groups A, B will be loaded with additional premises which are related to the case $A = \mathcal{A}_n, B = \mathcal{A}_{n+1}$. We define:

Definition 3. *A pair of finite abelian p -groups A, B is called a conic transition, if the following hold:*

1. A, B are abelian p -groups written additively and $N : B \rightarrow A$ and $\iota : A \rightarrow B$ are linear maps which are surjective, respectively injective. Moreover $N \circ \iota = p$ as a map $B \rightarrow B$. The ranks are $r = p\text{-rk}(A) \leq r' = p\text{-rk}(B)$. Note that for $r = r'$ we are in the case of Lemma 5, so this will be considered as a stable case.

2. There is a finite cyclic p -group $G = \mathbb{Z}_p\tau$ acting on A and B , making B into cyclic $\mathbb{Z}_p[\tau]$ -modules. We let $T = \tau - 1$.
3. We assume that there is a polynomial $\omega(T) \in \mathbf{R} := \mathbb{Z}/(p^N \cdot \mathbb{Z})[T]$, for $N > 2 \exp(B)$, with

$$N = \frac{(\omega(T) + 1)^p - 1}{\omega} \in \mathbf{R},$$

$$\omega \equiv T^{\deg(\omega)} \pmod{p\mathbb{Z}_p[T]}, \quad \text{and} \quad \omega \equiv 0 \pmod{T}.$$

In particular, (4) holds; we write $d = \deg(\omega(T)) \geq 1$. We also assume that $\omega A = 0$.

4. The kernel $K := \text{Ker}(N : B \rightarrow A) \subset B$ is assumed to verify $K = \omega B$ and if $x \in B$ verifies $\omega x = 0$, then $x \in \iota(A)$.
5. There is an $a \in A$ such that $a_i = T^i a, i = 0, \dots, r - 1$ form a \mathbb{Z}_p -base of A , and $a_0 = a$.

The transition is regular if $r' = pd$; it is regular flat, if $\text{sexp}(B) = \exp(B)$ and it is regular wild, if it is regular and $\exp(B) > \text{sexp}(B)$. It is initial if $r = d = 1$ and it is terminal if $r' < pd$. If $r = r'$, the transition is called stable. The module associated to the transition (A, B) is the transition module $\mathcal{T} = B/\iota(A)$. We shall write $\nu = \iota \circ N : B \rightarrow B$. Then $\nu = \nu(T)$ is a polynomial of degree $\deg(\nu) = (p - 1)d$ and $\omega\nu$ annihilates B .

We introduce some notions for the study of socles. Let $\varpi : B \rightarrow \mathbb{N}$ be the map $x \mapsto \text{ord}(x)/p$ and $\psi : B \rightarrow S(B)$ be given by $x \mapsto \varpi(x) \cdot x$, a \mathbb{Z}_p -linear map. Let $\Omega(b) = \{q_i := \varpi(T^i b) : i = 0, 1, \dots, r' - 1\}$. Then $q_0 \geq q_1 \geq \dots \geq q_{r'-1}$. The jumps of $\Omega(b)$ are the set

$$J := \{i : q_i > q_{i+1}\} \subset \{0, 1, \dots, r' - 2\}.$$

We shall write

$$B_j := \sum_{i=0}^j \mathbb{Z}_p T^i b \subset B, \quad 0 \leq j < r'.$$

We consider in the sequel only transitions that are not stable, thus we assume that $r < r'$. We show below that point 4 of the definition reflects the specific properties of conic modules, while the remaining ones are of general nature and apply to transitions in arbitrary cyclic Λ -modules. Throughout this chapter, a and b are generators of A and B as $\mathbb{Z}_p[T]$ -modules. Any other generators differ from a and b by units.

We start with an elementary fact which holds for finite cyclic $\mathbb{Z}_p[T]$ -modules X , such as the elements of conic transitions.

Lemma 7. *If (A, B) be a conic transition. If $y, z \in B \setminus pB$ are such that $y - z \in pB$, then they differ by a unit:*

$$(9) \quad y, z \notin pB, \quad y - z \in pB \quad \Rightarrow \quad \exists v(T) \in (\mathbb{Z}_p[T]^\times), \quad z = v(T)y.$$

Moreover, if $S(A), S(B)$ are $\mathbb{F}_p[T]$ -cyclic and $y \in B \setminus \{0\}$ is such that $Ty \in TS(B)$, then either $y \in S(B)$ or there are $a' \in \iota(a)$ and $z \in S(B)$ such that

$$(10) \quad y = z + a', \quad Ta' = 0, \quad \text{ord}(a') > p.$$

Proof. Let $b \in B$ generate this cyclic $\mathbb{Z}_p[T]$ module. Then $R(B) = B/pB$ is a cyclic $\mathbb{F}_p[T]$ module; since $\tau^{p^M} = 1$ for some $M > 0$, it follows that $(T + 1)^{p^M} - 1 = T^{p^M} = 0 \in \mathbb{F}_p[T]$, so the element T is nilpotent.

Let $y \in B$ with image $0 \neq \bar{y} \in R(B)$. Then there is a $k \geq 0$ such that $T^k b \mathbb{F}_p[T]R(B) = y \mathbb{F}_p[T]R(B)$: consider the annihilator ideal of the image $b' \in B/(pB, y)$. Since b is a generator, we also have $y = g(T)b, g \in \mathbb{Z}_p[T]$. The above shows that $g(T) \equiv 0 \pmod{T^k}$, so let $g(T) = T^k g_1(T)$ with $g_1(T) = \sum_{j \geq 0} c_j T^j$, $c_j \in \mathbb{Z}_p$. The above equality of ideals in B/pB implies that $c_0 \in \mathbb{Z}_p^\times$, since otherwise $T^k B \mathbb{F}_p[T]R(B) \supsetneq y \mathbb{F}_p[T]R(B)$. Therefore $g(T) \in (\mathbb{Z}_p[T])^\times$. Applying the same fact to y, z , we obtain (9) by transitivity.

Finally suppose that $0 \neq Ty \in S(B) = B[p]$. Then $y \neq 0$; if $\text{ord}(y) = p$ then $y \in S(B)$ and we are done. Suppose thus that $\text{ord}(y) = p^e, e > 1$ and let $y' = p^{e-1}y \in S(B)$. The socle $S(B)$ is $\mathbb{F}_p[T]$ cyclic, so there is a $z \in S(B)$ such that $Ty = Tz \in TS(B)$. Then $T(y - z) = 0$ and $y - z \in \iota(A)$ by point 4 of the definition 3; therefore $y = z + a', a' \in \iota(a)$. Moreover, $\text{ord}(y) = \text{ord}(a') > p$ while $Ty = Tz + Ta'$, thus $Ta' = 0$. This confirms (10). \square

2.5. Transition modules and socles. The following lemmata refer to conic transitions. We start with several results of general nature, which will then be used in the next section for a case by case analysis of transitions and minimal polynomials.

Lemma 8. *The following facts hold in conic transitions:*

- (i) *Suppose that $S(A)$ is $\mathbb{F}_p[T]$ -cyclic; then the socle $S(B)$ is also a cyclic $\mathbb{F}_p[T]$ -cyclic module.*
- (ii) *Let $x^\top = \{t \in \mathbb{Z}_p[T] : tx = 0\}$ be the annihilator ideal of x and $\bar{\omega} \in \mathbb{Z}_p[T]$ be a representant of the class $(\omega \bmod b^\top) \in B/b^\top$. We have*

$$(11) \quad \iota(S(A)) \subset S(K), \quad K \cap \iota(A) = \iota(S(A)), \quad \text{and}$$

$$(12) \quad K = \bar{\omega}B = a^\top B.$$

Proof. The point (i) follows from Lemma 3. Indeed, $S(B) \supseteq \iota(S(A))$ are elementary p -groups by definition. If $x \in S(B)[T]$, then $Tx = 0$ and point 3 of the definition of conic transitions implies that $x \in \iota(A) \cap S(B) = \iota(S(A))$. Thus $S(B)[T] \subseteq \iota(S(A))[T]$ and since $S(A)$ is $\mathbb{F}_p[T]$ cyclic, we know that $p\text{-rk}(\iota(S(A))[T]) = p\text{-rk}(S(B)[T]) = 1$. The Lemma 3 implies that the T -rank of $S(B)$ is one and $S(B)$ is cyclic as an $\mathbb{F}_p[T]$ -module.

Let now $x \in \iota(S(A))$, so $\omega x = px = 0$. Then $Nx = (pu + \omega^{p-1})x = 0$, and thus $x \in S(K)$. If $x' \in \iota(A) \cap K$, then $Nx' = px' = 0$ and thus $x' \in S(K) \cap \iota(A) = \iota(S(A))$, showing that (11) is true.

By point 4. of the definition of conic transitions, we have $K = \omega B = \omega \mathbb{Z}_p[T]b$ and since ω acts on b via its image modulo the annihilator of this generator, it follows that $K = \bar{\omega}b$ for any representant of this image in $\mathbb{Z}_p[T]$. For $t \in a^\top$ we have $N(tb) = tN(b) = ta = 0$; conversely, if $x = t'b \in K$, then $N(t'b) = t'N(b) = t'a = 0$ and thus $t' \in a^\top$. We thus have $K = a^\top B$, which confirms (12) and completes the proof of (ii). \square

An important consequence of the structure of the kernel of the norm is

Corollary 2. *Let (A, B) be a transition with $r < d$. Then $r' = r$.*

Proof. Let $\theta = T^r + pg(T) \in a^\top$ be a minimal annihilator polynomial of a . Then $\theta B \subset K = \bar{\omega}B$ so there is a $y \in \mathbb{Z}_p[T]$ such that $\theta b = \omega y b$ and since $\theta b \notin pB$, it follows that $y \notin p\mathbb{Z}_p[T]$. Let thus $y = cT^j + O(p, T^{j+1})$ with $j \geq 0$ and $(c, p) = 1$. Then

$$\alpha = T^r + pg(T) - \omega \cdot y = T^r + T^{d+j} + O(p, T^{d+j+1}) \in b^\top.$$

Using $d > r$, Weierstrass Preparation implies that there is a distinguished polynomial $h(T)$ of degree r and a unit $v(T)$ such that $\alpha = hv$. Since v is a unit, $h \in b^\top$. But then $T^r b \in P$ and thus $B = P$ and $p\text{-rk}(B) = r$, which confirms the statement of the Lemma. \square

The corollary explains the choice of the signification of flat and terminal transitions: a terminal transition can only be followed by a stable one.

We analyze in the next lemma the transition module \mathcal{T} in detail.

Lemma 9. *Let (A, B) be a conic transition and $\mathcal{T} = B/\iota(A)$ be its transition module. Then*

1. *The module \mathcal{T} is $\mathbb{Z}_p[T]$ -cyclic, annihilated by ν . and*

$$r' \leq r + (p-1)d.$$

Moreover

- (13) $\exp(B) \leq p \exp(A)$,
 and there is an $\ell(B)$ with $\text{ord}(T^{\ell-1}b) = \exp(B) = p \cdot \text{ord}(T^\ell B)$.
 2. If $S(A) \subset TA$ and $S(B)$ is folded, then $r' = r$.

Proof. Since $\nu(B) = \iota(A)$, it follows that $\nu(\mathcal{T}) = 0$, showing that $r' = p - \text{rk}(B) \leq p - \text{rk}(A) + p - \text{rk}(\mathcal{T}) \leq p - \text{rk}(A) + \deg(\nu) = r + (p-1)d$, which confirms the first claim in point 1.

Let now $q = \exp(A)$, so $q\iota(A) = 0$ and $qB \supseteq \iota(A)$. Thus $\mathcal{T}^\top \supseteq (B/qB)$. We let $\ell(B) = p - \text{rk}(B/qB)$ and prove the claims of the lemma. We have

$$pqu(T)b = -qT^{p-1}b + q\iota(a) = -qT^{p-1}b,$$

Assuming that $qT^{p-1}b \neq 0$, we obtain $p - \text{rk}(\mathcal{T}) \leq (p-1)d < p - \text{rk}(B/qB)$, in contradiction with the fact that B/qB is a quotient of \mathcal{T} . Therefore $qT^{p-1}b = 0$ and thus $pqu(T)b = 0$, so $\exp(B) = pq$. Therefore, the module $qB \subset S(B)$ and it has rank $\ell(B)$. Let $s' \in S(B)$ be a generator. Comparing ranks in the $\mathbb{F}_p[T]$ -cyclic module $S(B)$, we see that $T^{r'-\ell}s = qbv(T)$, $v(T) \in (\mathbb{F}_p[T])^\times$.

Suppose now that $S(B)$ is folded; then $\iota(S(A)) = T^k S(B)$, $k = r' - r$. If $s = Tg(T)\iota(a)$ is a generator of $\iota(S(A))$, then $T^{r'-r}s' = v(T)\iota(s)$, $v(T) \in (\mathbb{F}_p[T])^\times$. Thus

$$T(T^{r'-r-1}s' - g(T)v\iota(a)) = 0,$$

and by point 4 of the definition of conic transitions, $T^{r'-r-1}s' \in \iota(S(A))$. But then

$$r' = p - \text{rk}(S(B)) \leq p - \text{rk}(\iota(S(A))) + r' - (r+1) = r + r' - (r+1) = r' - 1.$$

This is a contradiction which implies that $r = r'$ and (A, B) is in this case a stable transition. \square

In view of the previous lemma, we shall say that the transition (A, B) is *wild* if $r' = pd$ and $S(B)$ is folded. The flat transitions are described by:

Lemma 10. *Let (A, B) be a conic transition. The following conditions are equivalent:*

- (i) *The exact sequence*

$$(14) \quad 0 \rightarrow \iota(A) \rightarrow B \rightarrow \mathcal{T} \rightarrow 0,$$

is split.

- (ii) *The jump-set $J(B) = \emptyset$,*
 (iii) *The socle $S(B)$ is straight,*

(iv) $\text{sexp}(B) = \exp(B)$,

Moreover, if (A, B) is a transition verifying the above conditions and $\exp(A) = q$, then $\exp(B) = q$.

Proof. The conditions (ii) and (iv) are obviously equivalent: if $q = \text{sexp}(B) = \exp(B)$, then the exponent $q_i = \text{ord}(T^i b) = q$ are all equal, and conversely, if these exponents are equal, then $\text{sexp}(B) = \exp(B)$: to see this, consider $x \in B \setminus pB$ such that $\text{ord}(x) = \text{sexp}(B)$. Since $0 \neq \bar{x} \in R(B)$, Lemma 7 shows that $x = T^k v(T)$, $k \geq 0$, $v \in (\mathbb{Z}_p[T])^\times$. Therefore $\text{ord}(x) = q_k = q$, as claimed.

Suppose that $S(B)$ is straight, so $\psi(b)$ generates $S(B)$. Then $T^j \psi(b) \neq 0$ for all $0 \leq j < r'$ and thus $T^j \varpi(b) \cdot b = \varpi(b)(T^j b) \neq 0$. Since $\text{ord}(\varpi(b)T^j b) \leq p$, it follows that the order is p and $\varpi(b) = \varpi(T^j b)$, so $\text{ord}(b) = \text{ord}(T^j b)$ for all j , and thus $\text{sexp}(B) = \exp(B)$. Hence (iii) \Rightarrow (ii), (iv). Conversely, suppose that the socle is folded. Then let $\psi(T^k b)$ be a generator of the socle, $k > 0$. The same argument as above shows that $\text{ord}(T^{k-1} b) > \text{ord}(T^k b)$ and thus $J(B) \neq \emptyset$. Therefore (ii) – (iv) are equivalent.

We show that (14) is split if (ii) – (iv) hold. Suppose that $\iota(a) \notin pB$; then $\iota(a) = \nu b$ has non trivial image in $R(B)$ and thus $\text{ord}(a) = \text{ord}(b)$. If (14) is not split, then $\psi(\iota(a)) \in \sum_{i=0}^{\deg(\nu)-1} \mathbb{Z}_p T^i b$, in contradiction to $S(B)$ being straight. Thus $J(b) = \emptyset$ implies (14) being split.

Conversely, we show that if (14) is split, then $S(B)$ is straight and $\text{sexp}(B) = \exp(B)$. We have $B = \iota(A) \oplus B_{r'-r-1}$ and $S(B) = S(B_{r'-r-1}) \oplus \iota(S(A))$. On the other hand, $\iota(S(A)) = \iota(A) \cap K \neq \emptyset$; therefore $S(B_{r-1}) \cap S(K) = \emptyset$, and it follows that $S(B)$ is straight. This completes the proof of the equivalence of (i) – (iv).

If $\exp(A) = q$ and the above conditions hold, then $\exp(B) = \text{sexp}(B)$ and thus $\ell(B) = p - \text{rk}(B) = r'$. We prove by induction that $r' = pd$: Assume thus that $p - \text{rk}(A) = d$ and let $s' = (q/p)b \in S(B)$, a generator. Then $s := Ns' = (q/b)\iota(a) \in \iota(S(A))$ will be a generator of $\iota(S(A))$. A rank comparison then yields

$$r' = p - \text{rk}(S(B)) = p - \text{rk}(S(A)) + (p - 1)d = pd.$$

From $\iota(a) = pbu(\omega) + \omega^{p-1}b$, we gather that $\text{ord}(a) \geq \max(p\text{ord}(b), \text{ord}(\omega^{p-1}b))$. Since $r' = p - \text{rk}(B) = pd$ and $\ell(B) = r'$, it follows that $\text{ord}(\omega^{p-1}b) = \text{ord}(b) = \text{ord}(a) = q$. The claim follows by induction on the rank of A . \square

We have seen in the previous lemma that regular flat transitions can be iterated indefinitely: this is the situation for instance in Λ -modules of unbounded rank: note that upon iteration, the exponent remains equal to the exponent of the first module and this may be any power

of p . The regular wild transitions will be considered below, after the next lemma that generalizes Lemma 5 to the case of increasing ranks, and gives conditions for a large class of terminal transitions.

Lemma 11. *Suppose that $q' := \text{ord}(a) > p$, $r' > r$ and $\iota(a) \in pB$. For $b \in B$ with $Nb = a$, we let the module $C = C(b) := \sum_{i=0}^{r-1} \mathbb{Z}_p T^i b$. Then*

$$(15) \quad C \supset \iota(A) \quad \text{and} \quad \iota(A) = pC.$$

2. *The element b spans B as a cyclic $\mathbb{Z}_p[T]$ -module and*

$$(16) \quad K = S(B).$$

Moreover, $r' \leq (p-1)d$ and the transition (A, B) is terminal.

Proof. Let $a' = \iota(a)$ and $c \in B$ be maximal and such that $p^e c = a'$, thus $T^i p^e c = T^i a'$. Let $C = \sum_{i=0}^{r-1} \mathbb{Z}_p T^i c$. Since $T^i a' = p^e T^i c$, we have $\iota(A) \subset C$ and thus $p\text{-rk}(C) \geq p\text{-rk}(A)$; on the other hand, the generators of C yield a base for C/pC , so the reverse inequality $p\text{-rk}(C) \leq p\text{-rk}(A)$ follows; the two ranks are thus equal.

We show that $N : C \rightarrow A$ is surjective. We may then apply the lemma 5 to the couple of modules A, C . Let $x \in \mathbb{Z}_p[T]$ be such that $N(c) = xa$. If $x \in (\mathbb{Z}_p[T])^\times$, then $N(x^{-1}c) = a$ and surjectivity follows.

Assume thus that $x \in \mathfrak{M} = (p, T)$. We have an expansion

$$N(c) = h(T)a = (h_0 + \sum_{i=1}^{r-1} h_i T^i)a, \quad h_i \in \mathbb{Z}_p,$$

and we assume, after eventually modifying h_0 by a p -adic unit, that $h_0 = p^k$ for some $k \in \mathbb{N}$. If $k = 0$, then $h(T) \in (\mathbb{Z}_p[T])^\times$, so we are in the preceding case, so $k > 0$. We rewrite the previous expansion as

$$(17) \quad N(c) = (p^k + Tg(T))a,$$

with $g(T) \in \mathbb{Z}_p[T]$ of degree $< r-1$. Let $f = e + k - 1$; from $p^e c = a$, we deduce:

$$p^f c = p^{k-1} \cdot (p^e c) = p^{k-1} a \quad \text{and} \quad N(p^f c) = N(p^{k-1} a) = p^k a.$$

By dividing the last two relations, we obtain $(1 - p^f)N(c) = Tg(T)a$. Since B is finite, we may choose $M > 0$ such that $p^{Mf} c = 0$. By multiplying the last expression with $(1 - p^{Mf})/(1 - p^f)$ we obtain

$$N(c) = Tg(T)(1 + p^f + \dots)a.$$

We compare this with (17), finding $Tg(T)(p^f + p^{2f} + \dots)a = p^k a$.

Since $\iota(a) \in pB$, we have $e > 0$. It follows that

$$p^k \cdot (1 - p^{e-1} Tg(T)(1 + p^f + \dots))a = 0,$$

so $p^k a = 0$ - since the expression in the brackets is a unit. Introducing this in (17), yields: $N(c) = Tg(T)a$. From $p^e c = a$, we then deduce $N(p^e c) = pa = p^e Tg(T)a$, and this yields $p(1 - p^{e-1}Tg(T))a = 0$. It follows from $e > 0$ that $pa = 0$, in contradiction with the hypothesis that $\text{ord}(a) > p$. We showed thus that if $\iota(a) \in pB$ and $\text{ord}(a) > p$, the norm $N : C \rightarrow A$ is surjective and we may apply the lemma 5. Thus $pC = A = N(C)$ and $pc = a$.

The module B is $\mathbb{Z}_p[T]$ -cyclic, so let b be a generator with $Nb = a$ and let $\tilde{C} = \sum_{i=0}^{r'-1} T^i c$. We claim that $\tilde{C} = B$. For this we compare $R(B)$ to $R(\tilde{C})$; we obviously have $R(\tilde{C}) \subseteq R(B)$. If we show that this is an equality, the claim follows from Nakayama's Lemma 2. The module $R(B)$ is $\mathbb{F}_p[T]$ cyclic, so there is an integer $k \geq 0$ with $\bar{c} \in T^k R(B)$. But then $N(\tilde{C}) \subset T^k N(B)$ and since $N : C \rightarrow A$ is surjective and $C \subset \tilde{C}$, we must have $k = 0$, which confirms the claim and completes the proof of point 1.

Note that $\iota(S(A)) \subset A = pC$, thus $C \cap K \supseteq \iota(S(A))$. Conversely, if $x \in C \cap K$, then $x \in pC$, since $T^i c \notin \iota(A)$ for $0 \leq i < r$, from the assumption $a \in pB$. Therefore $x \in pC \cap K = \iota(A) \cap K = \iota(S(A))$, as shown in (11), and

$$C \cap K = \iota(S(A)).$$

If $r' > r$, then $p\text{-rk}(K) = r' - r$; if $r = r'$, the transition is stable and $K \subset C$.

We now prove (16). Let $x = gb \in K$, $g \in a^\top \subset \mathbb{Z}_p[T]$. Since $pb \in A$, we have $px = gpb \in gA = 0$. Thus $K \subset S(B)$; conversely,

$$\begin{aligned} p\text{-rk}(S(B)) &= p\text{-rk}(S(A)) + r' - r = p\text{-rk}(S(A)) + (p\text{-rk}(B) - p\text{-rk}(C)) \\ &= p\text{-rk}(S(A)) + p\text{-rk}(K) \end{aligned}$$

and since $S(A) \subset K$ and $S(B)$ is cyclic, it follows that $S(B) = K$, which confirms (16) and assertion 2.

Finally, note that $p\text{-rk}(S(B)) = r'$ and since $\kappa = \omega b$ generates the socle and

$$0 = ((\omega + 1)^p - 1)b = \omega^{p-1}\kappa = T^{(p-1)d}\kappa,$$

it follows that $r' \leq (p-1)d$, as claimed. \square

We now investigate regular wild transitions and show that not more than two such consecutive transitions are possible.

Lemma 12. *Let (X, A) be a wild transition with $p\text{-rk}(X) = 1$ and (A, B) be a consecutive transition. Then*

1. $S(A) \not\subset K(A)$ and there is an $x' \in X$ with $\text{ord}(x') = p^2$ together with $g = Tf(T)a \in K(A)$ such that $s = \iota(x') + g$ is a generator of $S(A)$ and $\ell(A) = 2$.

2. The rank $r' \leq (p-1)d$ and B is terminal, allowing an annihilator $f_B(T) = T^{r'} - q/pw(T)$.

Proof. In this lemma we consider two consecutive transitions, so we write $T = \tau - 1$, acting on A, B and $\omega = (T+1)^p - 1$ annihilating A and acting on B . We shall also need the norm

$$\begin{aligned} \mathcal{N} &= N_{B/X} = \frac{1}{T}((T+1)^{p^2} - 1) = p^2U(T) + pT^pV(T), \\ U, V &= 1 + O(T) \in (\mathbb{Z}_p[T])^\times \end{aligned}$$

We let $q = \exp(A)$, $q/p = \exp(X)$ and $qp = \exp(B)$. In the wild transition (A, B) , the socle has length p and if $s \in B$ is a generator, then $0 \neq Ns = T^{p-1}s \in S(X)$; it follows that $s \notin K(A)$. Let $\iota(x) = Ns \in \iota(S(X))$; if $x \notin pX$, there is a $c \in \mathbb{Z}_p^\times$ with $T^{p-1}s = cN(a) = cpu(T)a + cT^{p-1}a$ and thus $T^{p-1}(s - ca)u^{-1}(T) = pa$; then $pa \in K(A) \cap \iota(S(X))$, and thus $\text{ord}(a) = p^2$ and Lemma 11 implies that $p\text{-rk}(A) < p$, which is a contradiction to our choice. Therefore $\exp(X) > p$ and there is an $x' \in X$ of order p^2 such that $p\iota(x') = N(\iota(x')) = N(s)$, so we conclude that $N(s - x') = 0$ and $x' - s \in K(A)$, which implies the first part in claim 1. We show now that $\ell(A) = 2$; indeed, $s - q/p^3\iota(x) \in K(A)$, so there is a power p^k such that $s - q/p^3\iota(x) = Tp^kw(T)b$ and $w \in \mathbb{Z}_p[T] \setminus p\mathbb{Z}_p[T]$. From $Ts = T^2p^kw(T)b$, and since $p\text{-rk}(Ts\mathbb{F}_p[T]) = p - 1$, we conclude that $w \in (\mathbb{F}_p[T])^\times$. Moreover the above identities in the socle imply

$$q/p^k \geq p^2 \text{ord}(Tp^ka) > p = \text{ord}(T^2p^ka) \geq \text{ord}(T^{p-1}p^ka) = q/p^{k+1}.$$

Consequently, $p^k = q/p^2$ and $\text{ord}(Ta) = q$ while $\text{ord}(T^2a) = q/p$, thus $\ell(A) = 2$.

For claim 2 we apply point 1. in Lemma 9. Let $q = \exp(A) = p\exp(X) > p^2$ and $\ell' = \ell(B) = p\text{-rk}(qB)$, $\ell = \ell(A) = p\text{-rk}(q/pA)$. From the cyclicity of the socle, we have

$$\begin{aligned} S(B)[T] &= q/p^2x\mathbb{F}_p = q/p^2\mathcal{N}(b)\mathbb{F}_p, \quad \text{hence } \exists c \in \mathbb{F}_p^\times, \\ (18) \quad T^{\ell'-1}qb &= cq/p^2\mathcal{N}(b) = (cqU(T) + cq/pT^pV(T))b. \end{aligned}$$

Assuming that $\ell' > 1$, then $qb(1 - O(T)) = q/pT^pV(T)b$ and thus $q/pT^pb = qbV_1(T)$. Then $\text{ord}(T^pb) = q$ and thus $\ell' < p$. Moreover $q/pT^{p+\ell'}b = qT^{\ell'}pV_1(T)b = 0$, thus $\text{ord}(T^{p+\ell'}b) \leq q/p$ and a fortiori

$$(19) \quad \text{ord}(T^{2p-1}b) \leq q/p, \quad \text{ord}(T^{p-1}b) \leq q.$$

We now apply the norm of the transition (A, B) , which may be expressed in ω as $N_{B/A} = pu(\omega) + \omega^{p-1}$. Note that $u(\omega) = v(T) \in$

$(\mathbb{Z}_p[T])^\times$, for some v depending on u . Also

$$\begin{aligned}\omega &= T^p + pTu(T) = T(T^{p-1} + pu(T)) \\ \omega^{p-1} &= T^{p(p-1)} + T^{(p-1)^2}p(p-1)u(T) + O(p^2).\end{aligned}$$

Since $p \geq 3$, (19) implies $\text{ord}(T^{p(p-1)}b) \leq q/p$ and $\text{ord}(T^{(p-1)^2}b) \leq q$. We thus obtain:

$$\begin{aligned}\iota(a) &= pv(T)b + (T^{p(p-1)} + pu_1(T)T^{(p-1)^2} + O(p^2))b, \quad \text{hence} \\ q/p\iota(a) &= qbv(T),\end{aligned}$$

and it follows in this case that $1 < \ell = \ell' = 2 < p$. Consider now the module $Q = \iota(A)/(\iota(A) \cap pB)$. Since $p\iota(A) \subset (\iota(A) \cap pB)$, this is an $\mathbb{F}_p[T]$ module; let T^i be its minimal annihilator. Then $T^i\iota(a)v_1(T) = pb, v_1 \in (\mathbb{Z}_p[T])^\times$; but $q/pv^{-1}(T)\iota(a) = qb$, and thus $q/p(T^i - v_2(T))\iota(a) = 0, v_2 \in (\mathbb{Z}_p[T])^\times$. If $i > 0$, then $v_2(T) - T^i \in (\mathbb{Z}_p[T])^\times$ and this would imply $q/p\iota(a) = 0$, in contradiction with the definition $q = \text{ord}(a)$. Consequently $i = 0$ and $\iota(a) \in pB$. We may thus apply the Lemma 11 to the transition (A, B) . It implies that the transition is terminal and $r' < (p-1)d$.

Finally we have to consider the case when $\ell' = 1$, so the relation (18) becomes

$$q(1/c - U(T))b = q/pT^pV(T)b.$$

If $c \neq 1$, then $q/pT^pb = qw(T), w \in (\mathbb{F}_p[T])^\times$ and the proof continues like in the case $\ell' > 1$. If $c = 1$, then we see from the development of $U(T) = 1 + T\binom{p^2}{2} + O(T)^2$ that there is a unit $d = \frac{p^2-1}{2} \in \mathbb{Z}_p^\times$ such that

$$qdTU_1(T)b = q/pT^pV(T)b = 0,$$

since $\ell = 1$ and thus $Tqb = 0$. We may deduce in this case also that $q/p\iota(a) = qb \cdot c_1, c_1 \in \mathbb{Z}_p^\times$ and complete the proof like in the previous cases. The annihilator polynomial of B is easily deduced from Lemma 11: $T^{r'}b \in \iota(S(A))$ is a generator of the last socle, so $T^{r'}b = Tq/p^2\iota(a) + cq/p^3\iota(x)$ and some algebraic transformations lead to

$$T^{r'}bw(T) = q/pb, \quad w \in (\mathbb{Z}_p[T])^\times,$$

which is the desired shape of the minimal polynomial. Note that $q/p = \exp(X)$; also, the polynomial is valid in the case when (A, B) is stable. We could not directly obtain a simple annihilating polynomial for A , but now it arises by restriction. \square

The previous lemma shows that an initial wild regular transition cannot be followed by a second one. Thus growth is possible over longer sequences of transitions only if all modules are regular flat. The

following lemma considers the possibility of a wild transition following flat ones.

Lemma 13. *Suppose that (A, B) is a transition in which A is a regular flat module of rank $p - \text{rk}(A) \geq p$ and $\exp(B) > \exp(A)$. Then B is terminal and $d < r' < (p - 1)d$. Moreover, there is a binomial $f_B(T) = \omega T^{r'-d} - qw(T) \in b^\top$; $w \in (\mathbb{F}_p[T])^\times$.*

Proof. Since $\exp(B) > \exp(A)$, the transition is not flat. Assuming that B is not terminal, then it is regular wild. Let $q = \exp(A) = \text{sexp}(A)$ and $s' \in S(B)$ be a generator of the socle of B . By comparing ranks, we have $T^{(p-1)d}s' = \omega^{p-1}s' = q/p\iota(a)v(T)$, $v \in (\mathbb{F}_p[T])^\times$. If $q = p$, then

$$T^{(p-1)d}s' = \nu v_1(T)b \Rightarrow \nu s' = pu(\omega)s' + \omega^{p-1}s' = \nu v_1(T)b,$$

and thus $s' - v_1(T)b \in K$. Since $K = \overline{\omega}B$, we have $(\overline{\omega}x + v_1(T))b \in S$. The factor $\overline{\omega}x + v_1(T) \in (\mathbb{Z}_p[T])^\times$ and it follows that $b \in S(B)$, which contradicts the assumption $\exp(B) > \exp(A)$, thus confirming the claim in this case. If $q > p$, then the previous identity yields $s' - q/p^2\iota(a) \in K$ and thus $s' = q/p^2\iota(a) + \omega xb$; we let $x = p^k v(T)$ with $v(0) \not\equiv 0 \pmod{p}$.

We assumed that $p - \text{rk}(S(B)) = pd$, so it thus follows that $v(T) \in (\mathbb{Z}_p[T])^\times$. Recall that $\text{ord}(b) = qp$ as a consequence of $\exp(B) > \exp(A)$ and (13); the norm shows that

$$qu(\omega)b + (q/p)\omega^{p-1}b = (q/p)\iota(a) \neq 0.$$

If $(q/p)\omega^{p-1}b = 0$, then $qu(\omega) = (q/p)\iota(a)$ which implies that the annihilator of $Q = \iota(A)/(pB \cap \iota(A))$ is trivial and $\iota(A) \subset pB$. We are in the premises of Lemma 11, which implies that B is terminal.

It remains that $\text{ord}(\omega^{p-1}b) = q$. We introduce this in the expression for the generator of the socle:

$$s' = \omega p^k v(T)b - q/pu(\omega)b - q/p^2\omega^{p-1}b \in S(B).$$

We have

$$q/p^{k-1} = \text{ord}(p^k b) \geq p^2 = \text{ord}(p^k \omega b) \geq \text{ord}(p^k \omega^{p-1}b) = q/p^k,$$

and thus $q/p^2 \leq p^k \leq q/p$. Note that

$$\omega s' = \omega^2 p^k v(T)b + \omega q/p^2 \iota(a) = \omega^2 p^k v(T)b \in S(B);$$

from $\omega^{p-1}(q/p)b \in S(B)$, it follows that $p^k = q/p$ and $\text{ord}(\omega b) = qp$ while $\text{ord}(\omega^2 b) = q = \text{ord}(\omega^{p-1}b)$. Let $i > 0$ be the least integer with $q/p\omega T^i b \in S(B)$. From the definition of s' we see that T^k is also the annihilator of $(q/p^2)\iota(a)$ in $\iota(A)/(S(\iota(A)))$, so $i = d$, since A is flat. It

follows that $\ell(B) = p - \text{rk}(B/qB) = 2d$ and the cyclicity of the socle implies that

$$T^{(p-2)d}s' = qbv_1(T) = T^{(p-2)d}s' = \frac{q}{p}\omega^{p-1}v(T)b + \frac{q}{p^2}\omega^{p-2}\iota(a).$$

Hence there is a unit $v_2(T) \in (\mathbb{Z}_p[T])^\times$ such that $\frac{q}{p}(p - \omega^{p-1}v_2(T))b = 0$. By comparing this with the norm identity $\frac{q}{p}(p + \omega^{p-1}u^{-1}(T))b = \frac{q}{p}\iota(a)$ we obtain, after elimination of $\omega^{p-1}b$, that $\frac{q}{p}(pbv_3(T) + \iota(a)) = 0$ and the reasonment used in the previous case implies that $\iota(a) \in pB$ so Lemma 11 implies that B is terminal.

We now show that $\iota(A) \subset pB$. Otherwise, $r' \geq (p-1)d$ and $T^{r'-1}s' = cT^{d-1}q/p\iota(a)$, so by cyclicity of the socle, $T^{r'-d}s' = v(T)q/p\iota(a)$ while $\nu s' = T^{pd-r'-1}\iota(a) \neq 0$. A similar estimation like before yields also in this case $s' = q/p\omega v(T)b + q/p^2T^j\iota(a)$, $j = pd - r' - 1$. Then $\omega^{p-2}s' = q/p\omega^{p-1}v(T)b \in S(B)$. Let $i > 0$ be the smallest integer with $pb \in \iota(a)$. Then $qb = T^i q/p\iota(a)v_1(T)$ and we find a unit $v_2(T)$ such that

$$q/p(\omega^{p-1}T^{i+r'-(p-1)d-1} - pv_2(T))b = 0.$$

This implies by a similar argument as above, that $\iota(a) \in pB$. Therefore we must have $r' < (p-1)d$ and $S(B) = K(B) \supset q/p\iota(A)$. Since $qb = q/p\iota(a) = \omega bT^{r'-d}v(T)$, we obtain an annihilator polynomial $f_B(T) = T^{r'-d} - qv^{-1}(T)$, which completes the proof of the lemma. \square

We finally apply the Lemma 10 to a sequence of flat transitions. This is the only case which allows arbitrarily large growth of the rank, while the value of the exponent is fixed to q .

Lemma 14. *Suppose that A_1, A_2, \dots, A_n are a sequence of cyclic $\mathbb{Z}_p[T]$ modules such that (A_i, A_{i+1}) are conic non-stable transitions with respect to some $\omega_i \in \mathbb{Z}_p[T]$ and $p - \text{rk}(A_1) = 1$. If $n > 3$, then A_i are regular flat for $1 \leq i < n$.*

Proof. If $n = 2$ there is only one, initial transition: this case will be considered in detail below. Assuming that $n > 2$, the transitions (A_i, A_{i+1}) are not stable; if (A_1, A_2) is wild, then Lemma 12 implies $n \leq 3$. The regular transitions being by definition the only ones which are not terminal, it follows that $A_k, k = 1, 2, \dots, n-1$ are flat. Lemma 13 shows in fact that A_2 , which must be flat, can only be followed by either a regular flat or a terminal transition. The claim follows by induction. \square

2.6. Case distinctions for the rank growth. We have gathered above a series of important building blocks for analyzing transitions. First we have shown in point 2. of Lemma 9 that all transitions that are not flat are terminal. Thus for the cases of interest that allow

successive growths of ranks, we must have $r = d, r' = pd$. The Lemma 10 shows that these reduce to $\exp(A) = q = \text{sexp}(A)$.

We start with an auxiliary result which will be applied in both remaining cases:

Lemma 15. *Let (A, B) be a transition with $\exp(A) = p$ and $r = d < r' < pd$. Then $S(B) \supseteq K$ with equality for $r' \leq (p-1)d$. If $S(B) \neq K$, then $s = T^{pd-r'}$ is a generator of $S(B)$.*

Proof. Since $r = d = \deg(\omega)$, it follows that $N(T^i b) = T^i \iota(a) \neq 0$ for $i = 0, 1, \dots, r-1$ while $N(T^d b) = T^d \iota(a) = 0$, since $\exp(A) = p$. Therefore $K = \omega B$ and $R(K) = T^d R(B)$.

We first show that $S(B) \subset K$: let $s \in S(B)$ be a generator. Cyclicity of the socle implies that $T^{r'-1}s = c_0 T^{d-1} \iota(a) \neq 0, c_0 \in \mathbb{F}_p^\times$ and $T^{r'}s = 0$. We have $N(s) = (pu(\omega) + \omega^{p-1})s = \omega^{p-1}s = T^{(p-1)d}s$. If $r' \leq (p-1)d$, then $T^{(p-1)d}s = 0$ and thus $s \in K$ and $S(B) = S(K)$. Otherwise, $T^{(p-1)d}\bar{b} = \overline{\iota(a)} \in R(B)$ and a fortiori $N(s) \in \iota(S(A)) = \mathbb{F}_p[T]\iota(a)$. Let $0 \leq k < d$ be such that $N(s) = T^k \iota(a)$: we may discard an implicit unit by accordingly modifying s . Then $T^{d-(k+1)}N(s) \neq 0$ and $T^{d-k}N(s) = 0$. Therefore $T^{d-(k+1)}s \notin K = \omega B$ and $s \notin pB$. It follows that $\bar{s}R(B) = T^k R(B)$ and $s = T^k v(T)b$, by lemma 7. By comparing ranks, we see that $k = pd - r'$ and $s = T^{pd-r'}$ is a generator of $S(B)$. \square

For initial transitions we have:

Lemma 16. *Let (A, B) be a conic transition and suppose that $r = 1$ and the transition is terminal. If $r' < p$, then B has a monic annihilator polynomial $f_B(T) = T^{r'} - qw(T)$ with $q = \text{ord}(a)$ and $w \in (\mathbb{Z}_p[T])^\times$.*

Proof. We let $q = \text{ord}(a)$ throughout this proof. Assume first that $r' < p-1$, so $T^{p-1}b = T^{p-1-r'}(T^{r'}b) = 0$, since $T^{r'}a \in \iota(A)$ by definition of the rank. Then $\iota(a) = (pu(T) + T^{p-1})b = pu(T)b$ and $pb = u(T)^{-1}\iota(a) = \iota(a)$, since $u(T) \equiv 1 \pmod{T}$. We have thus shown that $\iota(a) \in pB$ and, for $q > p$, we may apply Lemma 11. It implies that $S(B) = K = TB$ and $T^{r'-1}(Tb) = cq/p\iota(a) = cqb, c \in \mathbb{Z}_p^\times$. This yields the desired result for this case. If $q = p$, the previous computation shows that $\iota(a) \in pB$, but Lemma 11 does not apply here. We can apply Lemma 15, and since, in the notation of the lemma, $d = 1$ and the transition is assumed not to be stable, we are in the case $1 < r' \leq p-d$ and thus $S(B) = K$ too. The existence of the minimal polynomial $f_B(T) = T^{r'} - pc \in b^\top$ follows from this point like in the case previously discussed.

If $r' = p-1$, then $T^{p-1}b = \iota(a) - pu(T)b$ and thus $T^p b = pTu(T)b = 0$ and $Tb \in S(B)$. Since the socle is cyclic and $K = TB$ it follows that

$K = S(B)$. In particular, there is a $c \in \mathbb{Z}_p^\times$ such that

$$\begin{aligned} T^{p-1}b &= \frac{cq}{p}\iota(a) = \frac{cq}{p}(pu(T) + T^{p-1})b \\ &= cqu(T)b + \frac{cq}{p}u(T)T^{p-1}b, \quad \text{hence} \\ T^{p-1}\left(1 - \frac{cq}{p}u(T)\right)b &= cqu(T)b. \end{aligned}$$

If $q > p$, then $1 - \frac{cq}{p}u(T) \in (\mathbb{Z}_p[T])^\times$; if $q = p$, it must also be a unit: otherwise $1 - cu(T) \equiv 0 \pmod T$ and thus $T^pb = cqu(T)b = 0$, in contradiction with the fact that $qb = q/p\iota(a) \neq 0$. In both cases we thus obtain an annihilator polynomial of the shape claimed.

Finally, in the case $r' = p$ and the transition is wild. We refer to Lemma 12 in which treats this case in detail. \square

Remark 4. *Conic Λ -modules are particularly simple modules. The following example is constructed using Thaine's method used in the proof of his celebrated theorem [15]. Let $\mathbb{F}_1 \subset \mathbb{Q}[\zeta_{73}]$ be the subfield of degree 3 over \mathbb{Q} and $\mathbb{K}_1 = \mathbb{F}_1 \cdot \mathbb{Q}[\sqrt{-23}]$. Then $A_1 := (\mathcal{C}(\mathbb{K}_1))_3 = C_9$ is a cyclic group with 9 elements. If \mathbb{K}_2 is the next level in the cyclotomic \mathbb{Z}_3 -extension of \mathbb{K}_1 , then*

$$A_2 := (\mathcal{C}(K_2))_3 = C_{27} \times C_9 \times C_9 \times C_3 \times C_3 \times \times C_3.$$

The prime $p = 3$ is totally split in \mathbb{K}_1 and the classes of its factors have orders coprime to p . Although A_1 is \mathbb{Z}_p -cyclic, already A_2 has p -rank $2p$. Thus \mathbf{A} cannot be conic, and it is not even a cyclic Λ -module.

It is worth investigating, whether the result of this paper can extent to the case when socles are not cyclic and conicity is not satisfied, in one or more of its conditions. Can these tools serve to the understanding of Λ -modules as the one above?

3. TRANSITIONS AND THE CRITICAL SECTION

We return here to the context of Λ modules and conic elements, and use the notation defined in the introduction, so $\mathcal{A}_n = \Lambda a_n$ are the intermediate levels of the conic Λ -module $\Lambda a \subset \mathbf{A}^-$. We apply the results of the previous chapter to the transitions $C_n = (\mathcal{A}_n, \mathcal{A}_{n+1})$ for $n < n_0$. By a slight abuse of notation, we keep the additive notation for the ideal class groups that occur in these concrete transitions. The first result proves the consistency of the models:

Lemma 17. *Let the notations be like in the introduction and $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^-$ a conic element, $\mathcal{A} = \Lambda a$ and $\mathcal{A}_n = \Lambda a_n \subset A_n^-$. Then*

the transitions $(\mathcal{A}_n, \mathcal{A}_{n+1})$ are conic in the sense of Definition 3, for all $n > 0$.

Proof. Let $A = \mathcal{A}_n, B = \mathcal{A}_{n+1}$ and $N = \mathbf{N}_{\mathbb{K}_{n+1}, \mathbb{K}_n}, \iota = \iota_{n, n+1}$ be the norms of fields and the ideal lift map, which is injective since $a \in \mathbf{A}^-$. We let $T = \tau - 1$ with τ the restriction of the topological generator of Γ to \mathbb{K}_{n+1} and $\omega = \omega_n = (T + 1)^{p^{n-1}} - 1$. Then a fortiori $\omega A = 0$, and all the properties 1. - 3. of conic transitions follow easily. Point 5. is a notation. We show that the important additional property 4. follows from the conicity of a . The direction $\omega A \subset K$ follows from $Y_1 = TX$ in Theorem 2. The inverse inclusion is a consequence of point 1. of the definition of conic elements. Conversely, if $x \in K$, we may regard $x = x_{n+1} \in \mathcal{A}_{n+1}$ as projection of a norm coherent sequence $y = (x_m)_{m \in \mathbb{N}} \in \mathcal{A}$: for this we explicitly use point 3 of the definition of conic elements. Since $x = y_{n+1} = 1$ we have by point 2 of the same definition, $y \in \omega_n \cdot \mathcal{A}$. This implies $y_n = Nx = 1$; this is the required property 4 of Definition 3 \square

The next lemma relates $v_p(a_1)$ to the minimal polynomials $f_a(T)$:

Lemma 18. *Let $a \in \mathbf{A}^-$ be conic and $m = v_p(a_1)$. Then $v_p(f_a(0)) = m$. In particular, if $v_p(a_1) = 1$, then $f_a(T)$ is an Eisenstein polynomial.*

Proof. Let $q = p^m$ and $b = qa \in \Lambda a$. Then $b_1 = 0$ and, by conicity, it follows that $qa = b = Tg(T)a$. It follows that $Tg(T) - q$ annihilates a . We may choose g such that $\deg(g(T)T) = \deg(f_a(T))$, so there is a constant $c \in \mathbb{Z}_p$ such that $Tg(T) - q = cf_a(T)$. Indeed, if c is the leading coefficient of $Tg(T)$, the polynomial $D(T) = Tg(T) - q - cf_a(T)$ annihilates a and has degree less than $\deg(f_a)$. Since f_a is minimal, either $D(T) = 0$, in which case $c = 1$ and $f_a(T) = Tg(T) - q$, which confirms the claim, or $D(T) \in p\mathbb{Z}_p[T]$ and $c \equiv 1 \pmod{p}$. Since c is a unit in this case, we may replace b by $c^{-1}b = Tg_1(T)a$ and the polynomial $Tg(T)$ is now monic. The previous argument implies that $f_a(T) = Tg_1(T) - c^{-1}q$, which completes the proof. Since $f_a(T)$ is distinguished, we have $f_a(T) \equiv T^d \pmod{p}$ and if $m = 1$, then $p^2 \nmid f_a(0)$, so $f_a(T)$ is Eisenstein. The converse is also true. \square

If $m > 1$, we have seen in the previous chapter that there are minimal polynomials of \mathcal{A}_{n_0} which are essentially binomials; in particular, they are square free. It would be interesting to derive from this fact a similar conclusion about $f_a(T)$. We found no counterexamples in the tables in [6]; however the coefficients of $f_{n_0}(T)$ are perturbed in the stable growth too, and there is no direct consequence that we may derive in the present setting. The next lemma describes the perturbation of minimal polynomials in stable growth:

Lemma 19. *Let $g_n(T) = T^r - p\tilde{g}_n(T)$ be a minimal polynomial of \mathcal{A}_n . If $n \geq n_0$, then*

$$(20) \quad g_n(T) \equiv f_a(T) \pmod{\mathcal{A}_{n-1}^\top}$$

Proof. The exact annihilator $f_a(T)$ of \mathcal{A} also annihilates all finite level modules \mathcal{A}_n . In particular, for $n \geq n_0$ we have $\deg(g_n(T)) = \deg(f_a)$ for all minimal polynomials g_n of \mathcal{A}_n , and thus $\deg(g_n - f_a) < \lambda(a)$. We note that $g_n - f_a = p\delta_n(T) \in p\mathbb{Z}_p[T]$ with $\deg(\delta_n) < r$. It follows that

$$0 = p\delta_n(T)a_n = \delta_n(T)\iota_{n-1,n}(a_{n-1}),$$

and since ι is injective, it follows that $\delta_n(T) \in \mathcal{A}_{n-1}^\top$, as claimed. \square

It is worthwhile noting that if a is conic and $f_a(T) = \prod_{i=1}^k f_i^{e_i}(T)$ with distinct prime polynomials $f_i(T)$, then $b_i := f_a(T)/f_i(T)a$ have also conic transitions, but the modules Λb_i are of course not complementable as Λ -modules.

3.1. Proof of Theorem 1. With this, we shall apply the results on conic transitions and prove the Theorem 1

Proof. Let $a \in \mathbf{A}^- \setminus p\mathbf{A}^-$ be conic, let n_0 be its stabilization index and $\mathcal{A}_n = \Lambda a_n, n \geq 0$ be the intermediate levels of $\mathcal{A} = \Lambda a$. If $n_0 = 1$, then the Lemma 4 implies that $\lambda(a) = 1$ and $f_a(T)$ is linear. If $v_p(a_1) = 1$, then Lemma 18 implies that $f_a(T)$ is Eisenstein. Otherwise, the Lemmata 12 and 16 imply that $p - \text{rk}(\mathcal{A}) < p(p-1)$ with the exception of flat transition modules with high rank. The minimal polynomials at stabilization level are binomials, and this completes the proof. \square

3.2. Some examples. We shall discuss here briefly some examples⁴ drawn from the paper of Ernvall and Metsänkylä [6] and the tables in its supplement. The authors consider the primes $p = 3$, $\rho = \zeta_p$ and base fields $\mathbb{K} = \mathbb{K}(m) = \mathbb{Q}[\sqrt{m}, \rho]$. They have calculated the annihilator polynomials of $f_a(T)$ for a large choice of cyclic $A(\mathbb{K}(m))^-$. Here are some examples:

Example 1. *In the case $m = 2732$, $A^-(\mathbb{K}_1(m)) \cong C_{p^2}$ and $A^-(\mathbb{K}_2(m)) \cong C_{p^3} \times C_p$. The growth stabilizes and the polynomial $f_a(T)$ has degree 2; the annihilator $f_2(T)$ is a binomial, but not $f_a(T)$, so the binomial shape is in general obstructed by the term $f_a(T) = f_2(T) + O(p)$.*

⁴I am grateful to an anonymous referee for having pointed out some very useful examples related to the present topic.

Example 2. In the case $m = 3512$, we have $A^-(\mathbb{K}_1(m)) \cong C_{p^2}$ and $A^-(\mathbb{K}_2(m)) \cong C_{p^3} \times C_p \times C_p$. The polynomial $f_a(T)$ has degree 3 and for $B = A(\mathbb{K}_2(m))^-$ and $A = A(\mathbb{K}_1(m))^-$. This is a wild transition, which is initial and terminal simultaneously. We did not derive a precise structure for such transitions in Lemma 12.

Example 3. In the case $m = -1541$, the authors have found $\lambda = 4$. Unfortunately, the group $A(\mathbb{K}_3(m))$ cannot be computed with PARI, so our verification restricts to the structure of the transition $(A, B) = (\mathcal{A}_1, \mathcal{A}_2)$. This is the most interesting case found in the tables of [6] and the only one displaying a wild initial transition. The Lemma 12 readily implies that the transition $(\mathcal{A}_2, \mathcal{A}_3)$ must be terminal and $\lambda < (p-1)p = 6$, which is in accordance with the data. The structure is $\mathcal{A}_2 = C_{p^3} \times C_{p^3} \times C_p$ and with respect to this group decomposition we have the following decomposition of individual elements in $A = \mathcal{A}_1$ and $B = \mathcal{A}_2$:

$$\begin{array}{lll} b & = & (1, 0, 0) \quad Tb = (0, 10, 1) \quad T^2b = (-6, 9, 1) \\ T^3b & = & (18, -3, 0) \quad T^4b = (18, 9, 0) \quad T^5b = (0, 9, 0) \\ a & = & (0, 12, 1) \quad 3a = (0, 9, 0) \quad 9b = (9, 0, 0). \end{array}$$

Some of the particularities of this examples are: $S(B)$ is generated by $s' = T^3b - 2a$ and it is $\mathbb{F}_p[T]$ -cyclic, as predicted. Moreover, $s' \in K + \iota(A)$ but $s \notin K$ and $pb \notin \iota(a)$, while $qb \in S(B)[T] = S(A)[T]$, both facts that were proved in the Lemma 12.

Example 4. In all further examples with $\lambda \geq 3$, the fields $\mathbb{K}(m)$ have more than one prime above p and $\mathbf{A}^-(m)$ is not conic. For instance, for $m = 2516$, we also have $A^-(\mathbb{K}_1(m)) \cong C_{p^2}$ and $A^-(\mathbb{K}_2(m)) \cong C_{p^3} \times C_p \times C_p$, but $T^3b = 0$, for b a generator of $A(\mathbb{K}_2(m))^-$. The module is thus obviously not conic. This examples indicate a phenomenon that was verified in more cases, such as our example in Remark 4: an obstruction to conicity arises from the presence of floating elements $b \in \mathbf{A}^-$. These are defined as sequences $b = (b_n)_{n \in \mathbb{N}} \in \mathbf{A}^- \setminus (p, T)\mathbf{A}^-$ having $b_1 = 0$. When such elements are intertwined in the structure of Λ_a , one encounters floating elements. It is an interesting question to verify if the converse also holds: $a \in \mathbf{A}^- \setminus (p, T)\mathbf{A}^-$ is conic if it contains not floating elements. Certainly, the analysis of transitions in presence of floating elements is obstructed by the fact that the implication $Tx = 0 \Rightarrow x \in A$ is in general false. However, the obstruction set is well defined by the submodule of floating elements, which indicates a possible extension of the concepts developed in this paper. The analysis of floating elements is beyond the scope of this paper and will be undertaken in subsequent research.

Example 5. Let $\mathbb{K} = \mathbb{Q}[\sqrt{-31}]$ with $A(\mathbb{K}) = C_3$ and only one prime above $p = 3$. A PARI computation shows that $A(\mathbb{K}_2) = C_{p^2}$, so Fukuda's Theorem implies that \mathbf{A} is Λ -cyclic with linear annihilator. Let \mathbb{L}/\mathbb{K} be the cyclic unramified extension of degree p . There are three primes above p in \mathbb{L} and $A(\mathbb{L}) = \{1\}$, a fact which can be easily proved and needs no verification. Let $\mathbb{L}_n = \mathbb{L} \cdot \mathbb{K}_n$ be the cyclotomic \mathbb{Z}_p -extension of \mathbb{L} . One can also prove that $A(\mathbb{L}_n) \cong (A_n(\mathbb{K}))^p$, so $\mathbf{A}(\mathbb{L})$ is also Λ cyclic with the same linear annihilator polynomial as $\mathbf{A}(\mathbb{K})$. Let $b \in \mathbf{A}(\mathbb{L})$ be a generator of the Λ -module. The above shows that b is a floating class.

The extension \mathbb{L}/\mathbb{Q} in this example is galois but not CM and p splits in \mathbb{L}/\mathbb{K} in three principal primes. If $\nu \in \text{Gal}(\mathbb{L}/\mathbb{K})$ is a generator, it lifts in $\text{Gal}(\mathbb{H}_\infty/\mathbb{K})$ to an automorphism $\tilde{\nu}$ that acts non trivially on $\text{Gal}(\mathbb{H}_\infty/\mathbb{L}_\infty)$.

Let \mathbb{B}_∞ be the \mathbb{Z}_p -extension of \mathbb{Q} and \mathbb{H}_∞ be the maximal p -abelian unramified extension of \mathbb{K}_∞ and of \mathbb{L}_∞ (the two coincide in this case); then the sequence

$$(2\mathfrak{D}) \rightarrow \text{Gal}(\mathbb{L}_\infty/\mathbb{B}_\infty) \rightarrow \text{Gal}(\mathbb{H}_\infty/\mathbb{B}_\infty) \rightarrow \text{Gal}(\mathbb{H}_\infty/\mathbb{L}_\infty) \rightarrow 0$$

is not split in the above example, and this explains why $\tilde{\nu}$ lifts to a generator of $X' := \text{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty)$.

Let $\mathfrak{p}, \nu\mathfrak{p}, \nu^2(\mathfrak{p}) \subset \mathbb{L}$ be the primes above p and $I_0, I_1, I_2 \subset \text{Gal}(\mathbb{H}_\infty/\mathbb{L})$ be their inertia groups: then $I_1 = I_0^{\tilde{\nu}}, I_2 = I_0^{\tilde{\nu}^2}$. Let $I \subset \text{Gal}(\mathbb{H}_\infty/\mathbb{K})$ be the inertia of the unique prime above p and $\tau \in \text{Gal}(\mathbb{H}_\infty/\mathbb{K})$ be a generator of this inertia. We fix τ' as a lift of the topological generator of Γ : it acts in particular also on \mathbb{L} . Let τ be a generator of I_0 and $a \in X = \text{Gal}(\mathbb{H}_\infty/\mathbb{L}_\infty)$ such that $\tau_1 = a\tau$ is a generator of I_1 . We assume that both τ, τ_1 restrict to a fixed topological generator of $\Gamma = \text{Gal}(\mathbb{L}_\infty/\mathbb{K}_\infty)$. Then

$$\tau_1 = a\tau = \tau^{\tilde{\nu}} = \tilde{\nu}^{-1}\tau\tilde{\nu} \quad \Rightarrow \quad a = \tilde{\nu}^{-1}\tau\tilde{\nu}\tau^{-1}.$$

Since τ acts by restriction as a generator of $\Gamma' = \text{Gal}(\mathbb{K}_\infty/\mathbb{K})$ and $\tilde{\nu}$ generates X' , the above computation implies that $a \in (\text{Gal}(\mathbb{H}_\infty/\mathbb{K}))' = TX' = pX' = X$. In particular, a is a generator of $X \cong \mathbf{A}(\mathbb{L})$.

In this case we have seen that the primes above p are principal, the module $\mathbf{A}(\mathbb{L})$ is floating and it is generated by $a = \tau_1\tau^{-1} \notin TX$. Thus $Y_1 = \Lambda a = \mathbb{Z}_p a$ and $[Y_1 : TX] = p$. Since TX is the commutator, there must be a cyclic extension \mathbb{L}'/\mathbb{L} of degree p which is p -ramified but becomes unramified at infinity. It arises as follows: let \mathbb{H}_2 be the Hilbert class field of \mathbb{K}_2 . Then $\mathbb{H}_2/\mathbb{L}_2$ is cyclic of degree p and $\text{Gal}(\mathbb{H}_2/\mathbb{K}) = \langle \varphi(a_2) \rangle$, with $a_2 \in A(\mathbb{K}_2)$ a generator. Thus $(T - cp)a_2 = 0$ for some $c \in \mathbb{Z}_p^\times$ and $\text{Gal}(\mathbb{H}_2/\mathbb{L}_2) = p \langle \varphi(a_2) \rangle = \langle \varphi(Ta_2) \rangle$. Since

$T^2 a_2 = c^2 p^2 a_2$, it follows that $T \text{ Gal } (\mathbb{H}_2/\mathbb{L}_2) = 0$ and thus $\mathbb{H}_2/\mathbb{L}_1$ is abelian. This induces a cyclic extension $\mathbb{L}'_1/\mathbb{L}_1$ which is p -ramified, but becomes unramified already over \mathbb{L}_2 .

It also explains the role of the sequence (21) in Theorem 3. Phenomena in this context will be investigated together with the question about floating classes in a subsequent paper.

The prime $p = 3$ is interesting since it immediately display the more delicate cases $r' = p - 1$ and $r = p$ in Lemma 16. We found no examples with $\lambda > p$, which require an intermediate flat transition according to the above facts.

4. THE RAMIFICATION MODULE

In this section we prove the theorems stated in §1.2. The terms and notations are those introduced in that introductory section. Note that the choice of \mathbb{K} as a galois CM extension containing the p -th roots of unity is useful for the simplicity of proofs. If \mathbb{K} is an arbitrary totally real or CM extension, one can always take its normal closure and adjoin the roots of unity: in the process, no infinite modules can vanish, so facts which are true in our setting are also true for subextensions of \mathbb{K} verifying our assumptions.

Let us first introduce some notations: \mathbb{H}_1 is the p -part of the Hilbert class field of \mathbb{K} and $\overline{\mathbb{H}}_1 = \mathbb{H}_1 \cdot \mathbb{K}_\infty$; Ω/\mathbb{K} is the maximal p -abelian p -ramified extension of \mathbb{K} . It contains in particular \mathbb{K}_∞ and $\mathbb{Z}_p\text{-rk}(\Omega/\mathbb{H}_1) = r_2 + 1 + \mathcal{D}(\mathbb{K})$, where $\mathcal{D}(\mathbb{K})$ is the Leopoldt defect. Since \mathbb{K} is CM, complex multiplication acts naturally on $\text{Gal } (\Omega/\mathbb{K}_\infty)$ and induces a decomposition

$$\text{Gal } (\Omega/\mathbb{K}_\infty) = \text{Gal } (\Omega/\mathbb{K}_\infty)^+ \oplus \text{Gal } (\Omega/\mathbb{K}_\infty)^-;$$

this allows us to define

$$(22) \quad \begin{aligned} \Omega^- &= \Omega^{\text{Gal}(\Omega/\mathbb{K}_\infty)^+} \\ \Omega^+ &= \Omega^{\text{Gal}(\Omega/\mathbb{K}_\infty)^-}, \end{aligned}$$

two extensions of \mathbb{K}_∞ .

We shall review Kummer radicals below and derive a strong property of galois groups which are Λ -modules with annihilator a power of some polynomial: the order reversal property. Combined with an investigation of the galois group of Ω^-/\mathbb{H}_1 by means of class field theory, this leads to the proof of Theorem 3.

4.1. Kummer theory, radicals and the order reversal. Let \mathbf{K} be a galois extension of \mathbb{Q} which contains the p -th roots of unity and \mathbb{L}/\mathbf{K} be a finite Kummer extension of exponent $q = p^m, m \leq n$. Its classical Kummer radical $\text{rad}(\mathbb{L}/\mathbf{K}) \subset \mathbf{K}^\times$ is a multiplicative group containing $(\mathbf{K}^\times)^q$ such that $\mathbb{L} = \mathbf{K}[\text{rad}(\mathbb{L})^{1/q}]$ (e.g. [14], Chapter VIII, §8). Following Albu [1], we define the *cogalois* radical

$$(23) \quad \text{Rad}(\mathbb{L}/\mathbf{K}) = ([\text{rad}(\mathbb{L}/\mathbf{K})^{1/q}]_{\mathbf{K}^\times}) / \mathbf{K}^\times,$$

where $[\text{rad}(\mathbb{L}/\mathbf{K})^{1/q}]_{\mathbf{K}^\times}$ is the multiplicative \mathbf{K}^\times -module spanned by the roots in $\text{rad}(\mathbb{L}/\mathbf{K})^{1/q}$ and the quotient is one of multiplicative groups. Then $\text{Rad}(\mathbb{L}/\mathbf{K})$ has the useful property of being a finite multiplicative group isomorphic to $\text{Gal}(\mathbb{L}/\mathbf{K})$. For $\rho \in \text{Rad}(\mathbb{L}/\mathbf{K})$ we have $\rho^q \in \text{rad}(\mathbb{L}/\mathbf{K})$; therefore, the Kummer pairing is naturally defined on $\text{Gal}(\mathbb{L}/\mathbf{K}) \times \text{Rad}(\mathbb{L}/\mathbf{K})$ by

$$\langle \sigma, \rho \rangle_{\text{Rad}(\mathbb{L}/\mathbf{K})} = \langle \sigma, \rho^q \rangle_{\text{rad}(\mathbb{L}/\mathbf{K})}.$$

Kummer duality induces a twisted isomorphism of $\text{Gal}(\mathbf{K}/\mathbb{Q})$ -modules $\text{Rad}(\mathbb{L}/\mathbf{K})^\bullet \cong \text{Gal}(\mathbb{L}/\mathbf{K})$. Here $g \in \text{Gal}(\mathbf{K}/\mathbb{Q})$ acts via conjugation on $\text{Gal}(\mathbb{L}/\mathbf{K})$ and via $g^* := \chi(g)g^{-1}$ on the twisted module $\text{Rad}(\mathbb{L}/\mathbf{K})^\bullet$; we denote this twist the *Leopoldt involution*. It reduces on $\text{Gal}(\mathbf{K}/\mathbb{K})$ to the classical Iwasawa involution (e.g. [13], p. 150).

We now apply the definition of cogalois radicals in the setting of Hilbert class fields. Let \mathbb{K} be like before, a CM galois extension of \mathbb{Q} containing the p -th roots of unity and we assume that, for sufficiently large n , the p^n -th roots are not contained in \mathbb{K}_{n-1} , but they are in \mathbb{K}_n . Let $\mathbb{L} \subset \mathbb{H}_\infty$ be a subextension with galois group $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty) = \varphi(M)|_{\mathbb{L}}$, with $M \subset \mathbf{A}$ a Λ -submodule which is \mathbb{Z}_p -free. Let $\mathbb{L}_n = \mathbb{L} \cap \mathbb{H}_n$ be the finite levels of this extension and let $z \in \mathbb{Z}$ be such that $\exp(M_n) = p^{n+z}$ in accordance with (7). If $z < 0$, we may take $z = \max(z, 0)$. We define $\mathbb{L}'_n = \mathbb{L}_n \cdot \mathbb{K}_{n+z}$, so that $\mathbb{L}'_n/\mathbb{K}_{n+z}$ is a Kummer extension and let $R_n = \text{Rad}(\mathbb{L}'_n/\mathbb{K}_{n+z})$ and $B_n \cong R_n^{p^{n+z}} \subset \mathbb{K}_n^\times / (\mathbb{K}_n^\times)^{p^{n+z}}$. Then 7 implies, by duality, that $R_{n+1}^p = R_n$, for $n > n_0$; the radicals form a norm coherent sequence both with respect to the dual norm $N_{m,n}^*$ and to the simpler p -map. Since $\mathbb{L} = \cup_n \mathbb{L}'_n$, we may define $\text{Rad}(\mathbb{L}/\mathbb{K}_\infty) = \varprojlim_n R_n$. The construction holds in full generality for infinite abelian extensions of some field containing $\mathbb{Q}[\mu_{p^\infty}]$, with galois groups which are \mathbb{Z}_p -free Λ -modules and projective limits of finite abelian p -groups. But we shall not load notation here for presenting the details. Also, the extension \mathbb{L} needs not be unramified, and we shall apply the same construction below for p -ramified extensions.

We gather the above mentioned facts for future reference in

Lemma 20. *Let $z \in \mathbb{N}$ be such that $\text{ord}(a_n) \leq p^{n+z}$ for all n and $\mathbb{K}'_n = \mathbb{K}_{n+z}$, $\mathbb{L}'_n = \mathbb{L}_n \cdot \mathbb{K}_{n+z}$. Then $\mathbb{L}'_n/\mathbb{K}'_n$ are abelian Kummer extensions with galois groups $\text{Gal}(\mathbb{L}'_n/\mathbb{K}'_n) \cong \varphi(M_n)$, galois over \mathbb{K} and with radicals $R_n = \text{Rad}(\mathbb{L}'_n/\mathbb{K}_{n+z}) \cong (\text{Gal}(\mathbb{L}'_n/\mathbb{K}_{n+z}))^\bullet$, as Λ -modules. Moreover, if $M = \Lambda c$ is a cyclic Λ -module, then there is a $\nu_{n+1,n}^*$ -compatible system of generators $\rho_n \in R_n$ such that $R_n^\bullet = \Lambda \rho_n$ and, for n sufficiently large, $\rho_{n+1}^p = \rho_n$. The system R_n is projective and the limit is $R = \varprojlim_n R_n$. We define*

$$\mathbb{K}_\infty[R] = \cup_n \mathbb{K}_{n+z}[R_n] = \mathbb{L}.$$

Note that the extension by the projective limit of the radicals R is a convention, the natural structure would be here an injective limit. However, this convention is useful for treating radicals of infinite extensions as stiff objects, dual to the galois group which is a projective limit. Alternatively, one can of course restrict to the consideration of the finite levels.

The order reversal is a phenomenon reminiscent of the inverse galois correspondence; if M is cyclic annihilated by $f^n(T)$, with f a distinguished polynomial, then there is an inverse correspondence between the f -submodules of M and the f^* submodules of the radical R . The result is the following:

Lemma 21. *Let $f \in \mathbb{Z}_p[T]$ be a distinguished polynomial and $a \in A^- \setminus A^p$ have characteristic polynomial f^m for $m > 1$ and let $\mathcal{A}_n = \Lambda a_n$, $\mathcal{A} = \Lambda$. Assume that $\mathbb{L} \subset \mathbb{H}_\infty$ has galois group $\Delta = \text{Gal}(\mathbb{L}/\mathbb{K}_\infty) \cong \mathcal{A}$ and let $R = \text{Rad}(\mathbb{L}/\mathbb{K}_\infty)$. At finite levels, we have $\text{Gal}(\mathbb{L}_n/\mathbb{K}_n) \cong \mathcal{A}_n$ and $R_n = \text{Rad}(\mathbb{L}'_n/\mathbb{K}_{n+z})$, with $R_n = \Lambda \rho_n$. Then*

$$(24) \quad \langle \varphi(a_n)^{f^k}, \rho_n^{(f^*)^j} \rangle_{\mathbb{L}'_n/\mathbb{K}_{n+z}} = 1 \quad \text{for } k+j \geq m.$$

Proof. Let $g = \varphi(a_n) \in \Delta_n$ be a generator and $\rho \in R_n$ generate the radical. The equivariance of Kummer pairing implies

$$\langle g^{f^k}, \rho^{(f^*)^j} \rangle_{\mathbb{L}'_n/\mathbb{K}_{n+z}} = \langle g, \rho^{(f^*)^{j+k}} \rangle = \langle g^{f^{j+k}}, \rho \rangle.$$

By hypothesis, $a_n^{f^m} = 1$, and using also duality, $g^{f^m} = \rho^{(f^*)^m} = 1$. Therefore, the Kummer pairing is trivial for $k+j \geq m$, which confirms (24) and completes the proof. \square

It will be useful to give a translation of (24) in terms of projective limits: under the same premises like above, writing $\rho = \varprojlim_n \rho_n$ for a generator of the radical $R = \text{Rad}(\mathbb{L}/\mathbb{K}_\infty)$, we have

$$(25) \quad \langle \varphi(a)^{f^k}, \rho^{(f^*)^j} \rangle_{\mathbb{L}/\mathbb{K}} = 1 \quad \text{for } k+j \geq m.$$

We shall also use the following simple result:

Lemma 22. *Let \mathbb{K} be a CM galois extension of \mathbb{Q} and suppose that $(\mathbf{A}')^-(T) \neq 0$. Then $\text{ord}_T(\mathbf{A}^-(T)) > 1$.*

Proof. Assuming that $(\mathbf{A}')^-(T) \neq 0$, there is some $a = (a_n)_{n \in \mathbb{N}} \in \mathbf{A}^-$ with image $a' \in (\mathbf{A}')^-[T]$. We show that $\text{ord}_T(a) = 2$. Let $\mathfrak{Q}_n \in a_n$ be a prime and n sufficiently large; then $\text{ord}(a_n) = p^{n+z}$ for some $z \in \mathbb{Z}$ depending only on a and not on n . Let $(\alpha_0) = \mathfrak{Q}^{p^{n+z}}$ and $\alpha = \alpha_0/\overline{\alpha_0}$; since $a' \in (\mathbf{A}')^-[T]$ it also follows that $a_n^T \in \mathbf{B}^-$ and thus $\mathfrak{Q}^T = \mathfrak{R}_n$ with $b_n := [\mathfrak{R}_n] \in \mathbf{B}_n$. If $b_n \neq 1$, then $\text{ord}_T(a) = 1 + \text{ord}_T(a') = 2$, and we are done.

We thus assume that $b_n = 1$ and draw a contradiction. In this case $\mathfrak{R}_n^{1-j} = (\rho_n)$ is a p -unit and $(\alpha^T) = (\rho_n^{p^{n+z}})$, so

$$\alpha^T = \delta \rho_n^{p^{n+z}}, \quad \delta \in \mu_{p^n}.$$

Taking the norm $N = N_{\mathbb{K}_n/\mathbb{K}}$ we obtain $1 = N(\delta)N(\rho_n)^{p^{n+z}}$. The unit $N(\delta) \in \mu(\mathbb{K}) = \langle \zeta_{p^k} \rangle$ – we must allow here, in general, that \mathbb{K} contains the p^k -th roots of unity, for some maximal $k > 0$. It follows that $\rho_1 := N(\rho_n)$ verifies $\rho_1^{p^{n+z}} = \delta_1$, and since $\delta_1 \notin E(\mathbb{K})^{p^{k+1}}$, it follows that $\rho_1^{p^k} = \pm 1$ and by Hilbert 90 we deduce that $\rho_n^{p^k} = \pm x^T$, $x \in \mathbb{K}_n^\times$. In terms of ideals, we have then

$$\begin{aligned} \mathfrak{Q}^{(1-j)Tp^{n+z}} &= (\alpha^T) = (x^{Tp^{n+z-k}}), \quad \text{hence} \\ \left(\mathfrak{Q}^{(1-j)p^k} / (x) \right)^{Tp^{n+z-k}} &= (1) \Rightarrow (\mathfrak{Q}^{(1-j)p^k} / (x))^T = (1). \end{aligned}$$

But \mathfrak{Q} is by definition not a ramified prime, so the above implies that a_n has order bounded by p^k , which is impossible since $a_n \in A_n^-$. This contradiction confirms the claim and completes the proof of the lemma. \square

4.2. Units and the radical of Ω . The extension Ω/\mathbb{K} is an infinite extension and $\mathbb{Z}_p\text{-rk}(\text{Gal}(\Omega/\mathbb{K})) = \mathcal{D}(\mathbb{K}) + r_2(\mathbb{K}_n) + 1$. Here $r_2(\mathbb{K}_n)$ is the number of pairs of conjugate complex embedding and the 1 stands for the extension $\mathbb{K}_\infty/\mathbb{K}$. Let $\wp \subset \mathbb{K}$ be a prime above p , let $D(\wp) \subset \Delta$ be its decomposition group and $C = \Delta/D(\wp)$ be a set of coset representatives in Δ . We let $s = |C|$ be the number of primes above p in \mathbb{K} . Moreover

$$\mathbb{Z}_p\text{-rk}(\text{Gal}((\Omega^-/\mathbb{K}_\infty))) = r_2(\mathbb{K}_n).$$

It is a folklore fact, which we shall prove constructively below, that the *regular* part $r_2(\mathbb{K}_n)$ in the above rank stems from $\Omega^- \subset \Omega_E$, where $\Omega_E = \cup_n \mathbb{K}_n[E_n^{1/p^n}]$. The radical is described precisely by:

Lemma 23. *Notations being like above, we define for $n > 1$: $\mathcal{E}'_n = \{e^{\nu_{n,1}^*} : e \in E_n\}$ and $\mathcal{E}_n = \mathcal{E}'_n \cdot (E_n)^{p^n}$. Then*

$$(26) \quad \Omega^- = \mathbb{H}_1 \cdot \cup_n \mathbb{K}_n[\mathcal{E}_n^{1/p^n}] \times \mathbb{T}_1,$$

where $\mathbb{T}_1/\mathbb{K}_1$ is an extension which shall be described in the proof. It has group $\text{Gal}(\mathbb{T}_1/\mathbb{K}_1) \cong (\mathbb{Z}/(p \cdot \mathbb{Z}))^{s-1}$.

Proof. We show that the subgroups \mathcal{E}_m give an explicite construction of Ω^- , as radicals. The proof uses reflection, class field theory and some technical, but strait forward estimations of ranks.

Let $U = \mathcal{O}(\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p)$ and $U^{(1)}$ be the units congruent to one modulo an uniformizor in each completion of \mathbb{K} at a prime above p . The global units $E_1 = E(\mathbb{K}_1)$ embed diagonally in U and we denote by \overline{E} the completion of this embedding, raised to some power coprime to p , so that $\overline{E} \subset U^{(1)}$. A classical result from class field theory [13] p. 140, says that

$$\text{Gal}(\Omega/\mathbb{H}_1) \cong U^{(1)}/\overline{E}.$$

Since $(U^{(1)})^- \cap \overline{E} = \mu_p$, it follows that $\text{Gal}(\Omega^-/\mathbb{H}_1^-) = (U^{(1)})^- \times \mathcal{T}(U^-)/\mu_p$, where the torsion part $\mathcal{T}(U^-) = \prod_{\nu \in C} \mu_p$ is⁵ the product of the images of the p -th roots of unity in the single completions, factored by the diagonal embedding of the global units.

For the proof, we need to verify that ranks are equal on both sides of (26). Let $\pi_\nu \in \mathbb{K}_n$ be a list of integers such that $(\pi_\nu) = \wp^{\nu h}$ for h the order of the class of \wp^ν in the ideal class group $\mathcal{C}(\mathbb{K})$. Then we identify immediately $\mathbb{T}_1 = \prod_{\nu \in C} \mathbb{K}[\pi_\nu^{1/p}]$ as a p -ramified extension with group $\text{Gal}(\mathbb{T}_1/\mathbb{K}) = \mathcal{T}(U^-)/\mu_p \subset \text{Gal}(\Omega^-/\mathbb{H}_1^-)$.

A straight forward computation in the group ring yields that $T^*x \equiv 0 \pmod{(\omega_n, p^n)\Lambda}$ iff $x \in \nu_{n,1}^* \Lambda$. On the other hand, suppose that $x \in \text{rad}(\Omega^-/\mathbb{K}_n) \cap E_n$; note that here the extensions can be defined as Kummer extensions of exact exponent p^n , so there is no need of an index shift as in the case of the unramified extensions treated above. This observation and Kummer theory imply that $x^{T^*} \in E_n^{p^n}$, and thus $x \in \mathcal{E}_n$. We denote as usual $\Omega_E = \cup_n \mathbb{K}_n[E_n^{1/p^n}]$. We found that $\cup_m \mathbb{K}_m[\mathcal{E}_m^{1/p^m}] = \Omega^- \cap \Omega_E$; by comparing ranks, we see that if $\Omega^- \neq \mathbb{T}_n \cdot \mathbb{H}_1 \cdot (\Omega^- \cap \Omega_E)$, then there is an extension $\Omega^- \supset \Omega'' \supsetneq (\Omega^- \cap \Omega_E)$, such that

$$\mathbb{Z}_p\text{-rk}(\text{Gal}(\Omega''/\mathbb{K}_\infty)) = r_2(\mathbb{K}) = \mathbb{Z}_p\text{-rk}(\text{Gal}(\Omega^- \cap \Omega_E)).$$

⁵We have assumed for simplicity that \mathbb{K} does not contain the p^2 -th roots of unity. The construction can be easily generalized to the case when \mathbb{K} contains the p^k -th but not the p^{k+1} -th roots of unity.

Since $\Omega_E \subset \overline{\Omega}$, where $\overline{\Omega}$ is the maximal p -abelian p -ramified extension of \mathbb{K}_∞ , it follows that $\text{Gal}((\Omega^- \cap \Omega_E)/\mathbb{K}_\infty)$ is a factor of $\text{Gal}(\Omega^-/\mathbb{K}_\infty)$ and also of $\text{Gal}(\Omega''/\mathbb{K}_\infty)$.

The index $[\text{Gal}(\Omega'' : \mathbb{K}_\infty) : \text{Gal}((\Omega^- \cap \Omega_E)/\mathbb{K}_\infty)] < \infty$ and since $\text{Gal}(\Omega''/\mathbb{K}_\infty)$ is a free \mathbb{Z}_p -module and thus has no finite compact subgroups, it follows from infinite galois theory that $\Omega'' = \Omega^- \cap \Omega_E$, which completes the proof. \square

We note that for $\Omega_n \supset \mathbb{K}_n$, the maximal p -abelian p -ramified extension of \mathbb{K}_n , the same arguments lead to a proof of

$$(27) \quad \Omega_n^- = \cup_{m \geq n} \mathbb{K}_m [E(\mathbb{K}_m)^{N_{m,n}^*/p^m}].$$

4.3. Construction of auxiliary extension and order reversal.

On minus parts we have $\mathbb{Z}_p\text{-rk}(\Omega^-/\mathbb{K}^-) = r_2 + 1$ and the rank $\mathbb{Z}_p\text{-rk}(\Omega^-/\overline{\mathbb{H}}_1^-) = r_2$ does not depend on Leopoldt's conjecture. We let $G = \text{Gal}(\mathbb{H}_\infty/\mathbb{K})$ and $X = \varphi(\mathbf{A}) = \text{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty)$, following the notation in [16], Lemma 13.15. The commutator is $G' = TX$ and the fixed field $\mathbb{L} = \mathbb{H}_\infty^{TX}$ is herewith the maximal abelian extension of \mathbb{K} contained in \mathbb{H}_∞ . From the definition of Ω , it follows that $\mathbb{L} = \Omega \cap \mathbb{H}_\infty$ (see also [11], p. 257). Consequently $\text{Gal}(\mathbb{L}/\overline{\mathbb{H}}_1^-) \cong X/TX$. Let $F(T) = T^m G(T)$ be the annihilator polynomial of $p^M \mathbf{A}$, with p^M an annihilator of the \mathbb{Z}_p -torsion (finite and infinite) of \mathbf{A} . If \mathbf{A}° is this \mathbb{Z}_p -torsion, then $\mathbf{A} \sim \mathbf{A}(T) + \mathbf{A}(G(T)) + \mathbf{A}^\circ$.

From the exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 & \longrightarrow & p^\mu \mathbf{A}^- & \longrightarrow & p^\mu \mathbf{A}^-(T) + \mathbf{A}^-(G) & \longrightarrow & K_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & 0 & \longrightarrow & p^M \mathbf{A}^- & \longrightarrow & p^M \mathbf{A}^-(T) \oplus \mathbf{A}^-(G) & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

in which $M \geq \mu$ is such that annihilates the finite kernel and cokernel K_1, K_2 and the vertical arrows are multiplication by $p^{M-\mu}$, we see that it is possible to construct a submodule of \mathbf{A}^- which is a direct sum of G and T -parts. We may choose M sufficiently large, so that the following conditions also hold: $p^M \mathbf{A}^-(T)$ is a direct sum of cyclic Λ -modules and if a prime above p is inert in some \mathbb{Z}_p -subextension of $\mathbb{H}_\infty/\mathbb{H}_\infty^{p^M \varphi(\mathbf{A}^-)}$, then it is totally inert. Let $\tilde{\mathbb{K}} = \mathbb{H}_\infty^{p^M \varphi(\mathbf{A}^-)}$ for some M large enough to verify all the above conditions. Let $\mathbb{K}_T = \mathbb{H}_\infty^{p^M \mathbf{A}^-(G)}$; by construction, $\tilde{X}_T := \text{Gal}(\mathbb{K}_T/\tilde{\mathbb{K}}) \sim \mathbf{A}^-(T)$ and it is a direct sum of cyclic Λ -modules. Let $a_1, a_2, \dots, a_t \in p^M \mathbf{A}^-(T) = \varphi^{-1}(\tilde{X}_T)$ be such

that

$$(28) \quad \tilde{X}_T = \bigoplus_{j=1}^t \varphi(\Lambda a_i).$$

From the definition $\mathbb{K}_B^- = \Omega^- \cap \mathbb{H}_\infty \subset \mathbb{K}_T$ and Lemma 22 implies that $\text{Gal}(\mathbb{H}_\infty/\mathbb{K}_B^-) \sim \tilde{X}_T[T]$. Let now $a \in p^M \mathbf{A}^-(T) \setminus (p, T)p^M \mathbf{A}^-(T)$ - for instance $a = a_1$ and let $\mathcal{A} = \Lambda a$ while $\mathcal{C} \subset p^M \mathbf{A}^-(T)$ is a Λ -module with $\mathcal{A} \oplus \mathcal{C} = p^M \mathbf{A}^-(T)$. We assume that $m = \text{ord}_T(a)$ and let $b = T^{m-1}a \in \mathbf{A}^-[T]$. We define $\mathbb{K}_a = \mathbb{K}_T^{\varphi(\mathcal{C})}$, an extension with $\text{Gal}(\mathbb{K}_a/\tilde{\mathbb{K}}) \cong \mathcal{A}$. At finite levels we let $\mathbb{K}_{a,n} := \mathbb{K}_a \cap \mathbb{H}_n$ and let z be a positive integer such that $\mathbb{K}'_{a,n} := \mathbb{K}_{n+z} \mathbb{K}_{a,n}$ is a Kummer extension of $\mathbb{K}'_n := \mathbb{K}_{n+z}$, for all sufficiently large n - we may assume that M is chosen such that the condition $n > M$ suffices. The duals of the galois groups $\varphi(\mathcal{A}_n)$ are radicals $R_n = \text{Rad}(\mathbb{K}_{a,n}/\tilde{\mathbb{K}})$, which are cyclic Λ -modules too (see also the following section for a detailed discussion of radicals), under the action of Λ , twisted by the Iwasawa involution. We let $\rho_n \in R_n$ be generators which are dual to a_n and form a norm coherent sequence with respect to the p -map, as was shown above, since $n > M > n_0$; by construction, $\rho_n^{p^{n+z}} \in \mathbb{K}'_n$. We gather the details of this construction in

Lemma 24. *Notations being like above, there is an integer $M > 0$, such that the following hold:*

1. *The extension $\tilde{\mathbb{K}} := \mathbb{H}_\infty^{p^M X}$ has group $\tilde{X} := \text{Gal}(\mathbb{H}_\infty/\tilde{\mathbb{K}}) = \tilde{X}(T) \oplus \tilde{X}(G)$ below \mathbb{H}_∞ .*
2. *The extension $\mathbb{K}_T := \mathbb{H}_\infty^{\tilde{X}(G)}$ has group $\tilde{X}_T = \bigoplus_{i=1}^t \Lambda \varphi(a_i)$.*
3. *For $a \in p^M \mathbf{A}^-(T) \setminus (p, T)p^M \mathbf{A}^-(T)$ we define $\mathcal{A} = \Lambda a$ and let $\mathcal{C} \subset p^M \mathbf{A}^-(T)$ be a direct complement. We define $\mathbb{K}_a = \mathbb{H}_T^{\varphi(\mathcal{C})}$, so $\text{Gal}(\mathbb{K}_a/\tilde{\mathbb{K}}) = \varphi(\mathcal{A})$ and let $\mathbb{K}_{a,n} = \mathbb{K}_a \cap \mathbb{H}_n$.*
4. *There is a positive integer z such that for all $n > M$,*

$$\mathbb{K}'_{a,n} = \mathbb{K}_{n+z} \cdot \mathbb{K}_{a,n} \subset \mathbb{H}_{n+z}$$

is a Kummer extension of $\mathbb{K}'_n := \mathbb{K}_{n+z}$.

5. *For $\mathbb{K}_B^- = \Omega^- \cap \mathbb{H}_\infty$ we have $\mathbb{K}_B^- \subset \mathbb{K}_T$ and $\text{Gal}(\mathbb{H}_\infty/\mathbb{K}_B^-) \sim \tilde{X}_T[T]$.*
6. *The radical $R_n = \text{Rad}(\mathbb{K}_{a,n}/\tilde{\mathbb{K}}) \cong \mathcal{A}_n^\bullet$ and we let $\rho_n \in R_n$ generate this radical as a Λ^* -cyclic module, so that $\rho_n^{(T^*)^i}$, $i = 0, 1, \dots, m-1$ form a dual base to the base $a_n^{T^i}$, $i = 0, 1, \dots, m-1$ of \mathcal{A}_n . We have $\rho_n^{p^{n+z}} \in \mathbb{K}'_n$.*

We may apply the order reversal to the finite Kummer extensions $\mathbb{K}_{a,n}/\tilde{\mathbb{K}}_n$ defined in Lemma 24. In the notation of this lemma, we assume that $m = \text{ord}_T(a) > 1$. We deduce from 24 that

$$\langle \varphi(d_n^{29}), \rho_n^{(T^*)^{m-1-i}} \rangle_{\mathbb{K}_{a,n}/\tilde{\mathbb{K}}} = \zeta_{p^v},$$

$$v \geq n + z - M, \quad i = 0, 1, \dots, m-1.$$

This fact is a direct consequence of (24) for $i = 0$ and it follows by induction on i , using the following fact. Let $\mathbb{F}_i = \tilde{\mathbb{K}}[\rho_n^{(T^*)^{m-1-i}}]$; then $\overline{\mathbb{F}}_i = \prod_{j=0}^i \mathbb{F}_j$ are galois extensions of $\tilde{\mathbb{K}}_1$ and in particular their galois groups are Λ -modules. In particular, $\text{Gal}(\mathbb{F}_{m-1}/\tilde{\mathbb{K}}) \cong \mathcal{A}_n^{T^{m-1}} = \mathcal{A}_n[T]$. From Lemma 22 we know that $\mathcal{A}_n[T] \subset \mathbf{B}_n^-$, so at least one prime $\mathfrak{p} \subset \tilde{\mathbb{K}}$ above p is inert in \mathbb{F}_{m-1} , and the choice of M in Lemma 24 implies that it is totally inert in $\mathbb{F}_{m-1}/\tilde{\mathbb{K}}_n$. Let $\wp \subset \mathbb{K}$ be a prime below \mathfrak{p} . It follows in addition $\overline{\mathbb{F}}_{m-2} \subset \mathbb{H}'_\infty \cdot \tilde{\mathbb{K}}$ and all the primes above p are split in $\overline{\mathbb{F}}_{m-2}$: this is because

$$\text{Gal}(\overline{\mathbb{F}}_{m-2}/\tilde{\mathbb{K}}) \cong \mathcal{A}_n/\mathcal{A}_n[T] = \mathcal{A}_n/(\mathcal{A}_n \cap \mathbf{B}_n) \subset \mathcal{A}'_n.$$

Let now \mathbb{K}_a be like above and $\mathbb{K}_b = \Omega^- \cap \mathbb{K}_a$, so $\mathbb{K}_b/\tilde{\mathbb{K}}$ is a \mathbb{Z}_p -extension. Moreover, we assume that $\mathbb{K}_b \not\subset \mathbb{H}'_\infty$, so not all primes above p are totally split. By choice of M , we may assume that there is at least on prime $\wp \subset \mathbb{K}$ above p , such that the primes $\tilde{K} \supset \mathfrak{p} \supset \wp$ are inert in \mathbb{K}_b . By the construction of Ω^- in the previous section, we have $T^*\text{Rad}(\mathbb{K}_b/\tilde{\mathbb{K}}) = 0$. The order reversal lemma implies then that $\text{Gal}(\mathbb{K}_b/\tilde{\mathbb{K}}) \cong \mathcal{A}/(T\mathcal{A})$. Assuming now that $m = \text{ord}_T(a) \geq 1$, the Lemma 22 implies that $T^{m-1}a \in \mathbf{B}^-$ and the subextension of \mathbb{K}_a which does not split all the primes above p is the fixed field of $T^{m-1}\mathcal{A}$; but then order reversal requires that $\text{Rad}(\mathbb{K}_b/\tilde{\mathbb{K}})$ is cyclic, generated by ρ , which is at the same time a generator of $\text{Rad}(\mathbb{K}_a/\tilde{\mathbb{K}})$ as a Λ -module. Since we have seen that $T^*\text{Rad}(\mathbb{K}_b/\tilde{\mathbb{K}}) = 0$, we conclude that $T^*\text{Rad}(\mathbb{K}_a/\tilde{\mathbb{K}}) = 0$, and by duality, $Ta = 0$. This holds for all $a \in p^M \mathbf{A}^-(T)$, so we have proved:

Lemma 25. *Let $\mathbb{H}_B^- = \Omega^- \cap \mathbb{H}_\infty$. If $[\mathbb{K}_B^- \cap \mathbb{H}'_\infty : \mathbb{K}_\infty] < \infty$, then $\mathbf{A}^-(T) = \mathbf{B}^-$.*

4.4. The contribution of class field theory. We need to develop more details from local class field theory in order to understand the extension $\mathbb{H}_B^- = \Omega^- \cap \mathbb{H}_\infty$. This is an unramified extension of \mathbb{K}_∞ which is abelian over \mathbb{H}_1 . We wish to determine the \mathbb{Z}_p -rank of this group and decide whether the extensions in \mathbb{H}_B^- split the primes above p or not.

Let $\wp \subset \mathbb{K}$ be a prime over p and $\wp^+ \subset \mathbb{K}^+$ be the real prime below it. If \wp^+ is not split in \mathbb{K}/\mathbb{K}^+ , then $\mathbf{B}^- = \{1\}$ and it is also known that $(\mathbf{A}')^-(T) = \{1\}$ in this case – this follows also from the Lemma 22. The case of interest is thus when \wp is split in \mathbb{K}/\mathbb{K}^+ . Let $D(\wp) \subset \Delta$ and C, s be defined like above and let $\mathfrak{p} \subset \Omega$ be a prime above \wp .

Local class theory provides the isomorphism $\text{Gal}(\Omega/\mathbb{H}_1) \cong U^{(1)}/\overline{E}$ via the global Artin symbol (e.g. [13],). We have the canonic, continuous embedding

$$\mathbb{K} \hookrightarrow \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{\nu \in C} \mathbb{K}_{\nu\wp},$$

and $U^{(1)} = \prod_{\nu \in C} U_{\nu\wp}^{(1)}$, where $U_{\mathfrak{p}}^{(1)}$ are the one-units in the completion at the prime \mathfrak{p} . The ring $U^{(1)}$ is a galois algebra and $\Delta = \text{Gal}(\mathbb{K}/\mathbb{Q}) \hookrightarrow \text{Gal}(U^{(1)}/\mathbb{Q}_p)$. Thus complex conjugation acts on $U^{(1)}$ via the embedding of \mathbb{K} and if $u \in U^{(1)}$ has $\iota_{\wp}(u) = x, \iota_{\overline{\wp}}(u) = y$, then ju verifies

$$\iota_{\wp}(ju) = \overline{y}, \quad \iota_{\overline{\wp}}(ju) = \overline{x}.$$

Moreover, $u \in U^-$ iff $u = v^{1-j}, v \in U$. Thus, if $\iota_{\wp}(v) = v_1$ and $\iota_{\overline{\wp}}(v) = v_2$, then

$$(30) \quad \iota_{\wp}(u) = v_1/\overline{v_2}, \quad \iota_{\overline{\wp}}(u) = v_2/\overline{v_1} = 1/\overline{\iota_{\wp}(u)}.$$

One can analyze U^+ in a similar way. Note that \mathbb{Z}_p embeds diagonally in U^+ ; this is the preimage of $\text{Gal}(\mathbb{K}_{\infty}/\mathbb{K})$, under the global Artin symbol.

Next we shall construct by means of the Artin map some subextension of Ω^- which are defined uniquely by some pair of complex conjugate primes $\wp, \overline{\wp} \supset (p)$ and intersect \mathbb{H}_{∞} is a \mathbb{Z}_p -extension. Since $U^{(1)}$ is an algebra, there exists for each pair of conjugate primes $\wp, \overline{\wp}$ with fixed primes $\mathfrak{P}, \mathfrak{P}^j \subset \Omega$ above $(\wp, \overline{\wp})$, a subalgebra

$$(31) \quad \mathbb{M}_{\wp} = \{u \in U^{(1)} : \iota_{\mathfrak{P}}(u) = 1/\overline{\iota_{\mathfrak{P}^j}(u)}; \iota_{\nu\wp} = 1, \forall \nu \in C \setminus \{1, j\}\}.$$

Accordingly, there is an extension $\mathbb{M}_{\wp} \subset \Omega^-$ such that

$$\varphi^{-1}(\text{Gal}(\mathbb{M}_{\wp}/\mathbb{K}_{\infty})) = V_{\wp}.$$

By construction, all the primes above p above $\wp, \overline{\wp}$ are totally split in \mathbb{M}_{\wp} . Since $\text{Gal}(\mathbb{K}_{\wp}/\mathbb{Q}_p) = D(\wp)$ and U_{\wp} is a pseudocyclic \mathbb{Z}_p -module, pseudoisomorphic to $\mathbb{Z}_p[D(\wp)]$ (e.g. [13], p. 140-41), it follows that there is exactly one \mathbb{Z}_p -subextension $\mathbb{U}_{\wp} \subset \mathbb{M}_{\wp}$ with galois group fixed by the augmentation of $D(\wp)$. Since the augmentation and the norm yield a direct sum decomposition of $\mathbb{Z}_p[D(\wp)]$, this extension and its galois group are canonic – up to possible finite quotients. Locally, the completion of \mathbf{U}/\mathbb{Q}_p of \mathbb{U}_{\wp} at the primes above \wp is a \mathbb{Z}_p -extension of \mathbb{Q}_p , since its galois group is fixed $D(\wp)$. It follows by a usual argument

that $\mathbb{U}_\wp/\mathbb{K}_\infty$ is unramified at all primes above p , so $U_\wp \subset \mathbb{H}$. One has by construction that $\mathbb{U}_\wp^- \subset \Omega^-$, so we have proved:

Lemma 26. *Let \mathbb{K} be a CM extension like above and assume that the primes $\wp^+ \subset \mathbb{K}^+$ split in \mathbb{K}/\mathbb{K}^+ . For each prime $\wp \subset \mathbb{K}$ there is a canonic (up to finite subextensions) \mathbb{Z}_p -extension $\mathbb{U}_\wp \subset \Omega^- \cap \mathbb{H}_\infty$ such that $\text{Gal}(\mathbb{U}_\wp/\mathbb{K}_\infty) = \varphi \left(V_\wp^{\mathfrak{A}(\mathbb{Z}_p[D_\wp])} \right)$, where $\mathfrak{A}(\mathbb{Z}_p[D_\wp])$ is the augmentation ideal of this group ring and V_\wp is defined by (31). In particular, Ω^- contains exactly $s' = |C|/2$ unramified extensions.*

Our initial question boils down to the following: is $\mathbb{U}_\wp \subset \mathbb{H}'_\infty$?

The following example perfectly illustrates the question:

Example 6. *Let \mathbb{K}/\mathbb{Q} be an imaginary quadratic extension of \mathbb{Q} in which p is split. Then $U^{(1)}(\mathbb{K}) = (\mathbb{Z}_p^{(1)})^2$ and $\Omega = \mathbb{K}_\infty \cdot \Omega^-$ is the product of two \mathbb{Z}_p -cyclotomic extensions; we may assume that $\mathbb{H}_1 = \mathbb{K}$, so $\text{Gal}(\Omega/\mathbb{K}) = \varphi(U^{(1)}(\mathbb{K}))$. One may take the second \mathbb{Z}_p -extension in Ω also as being the anticyclotomic extension. In analyzing a similar example, Greenberg makes in [10] the following simple observation: since \mathbb{Q}_p has only two \mathbb{Z}_p -extensions and \mathbb{K}_∞ contains the cyclotomic ramified one, it remains that, locally $\Omega^-/\mathbb{K}_\infty$ is either trivial or an unramified \mathbb{Z}_p -extension. In both cases, $\Omega^- \subset \mathbb{H}_\infty$ is a global, totally unramified \mathbb{Z}_p -extension – we have used the same argument above in showing that $\mathbb{U}_\wp/\mathbb{K}_\infty$ is unramified. The remark settles the question of ramification, but does not address the question of our concern, namely splitting. However, in this case we know more. In the paper [9] published by Greenberg in the same year, he proves that for abelian extensions of \mathbb{Q} , thus in particular for quadratic ones, $(\mathbf{A}')^-(T) = \{1\}$. Therefore in this example, Ω^- cannot possibly split the primes above p .*

How can this fact be explained by class field theory?

We give here a proof of Greenberg's theorem [9] for imaginary quadratic extensions, and thus an answer to the question raised in the last example; we use the notations introduced there:

Proof. We shall write $\mathbb{L} = \mathbb{K}_\infty \cdot \mathbb{H}_1$; we have seen above that Ω/\mathbb{L} must be an unramified extension. Let $\mathfrak{P} \in \Omega$ be a prime above \wp , let $\tilde{j} \in \text{Gal}(\Omega/\mathbb{H}_1)$ be a lift of complex conjugation and let $\tau \in \text{Gal}(\Omega/\mathbb{H}_1)$ be a generator of the inertia group $I(\mathfrak{P})$: since $\Omega_\mathfrak{P}/\mathbb{K}_\wp$ is a product of \mathbb{Z}_p -extensions of \mathbb{Q}_p and \mathbb{Q}_p has no two independent ramified \mathbb{Z}_p -extensions, it follows that $I(\mathfrak{P}) \cong \mathbb{Z}_p$ is cyclic, so τ can be chosen as a topological generator. Then $\tau^j = j \cdot \tau \cdot j$ generates $I(\mathfrak{P}^j) \cong \mathbb{Z}_p$. Iwasawa's argument used in the proof of Theorem 2 holds also for Ω/\mathbb{H}_1 :

there is a class $a \in A_n$ with $\tau^j = \tau\varphi(a)$, where the Artin symbol refers to the unramified extension Ω/\mathbb{L} . Thus

$$j \cdot \tau \cdot j \cdot \tau^{-1} = \tau^{j-1} = \varphi(a).$$

The inertia groups $I(\mathfrak{P}) \neq I(\mathfrak{P}^j)$: otherwise, their common fixed field would be an unramified \mathbb{Z}_p -extension of the finite galois field \mathbb{H}_1/\mathbb{Q} , which is impossible: thus $\tau^{j-1} = \varphi(a) \neq 1$ generates a group isomorphic to \mathbb{Z}_p . Let now $\mathfrak{p} = \mathfrak{P} \cap \mathbb{L}$; the primes $\mathfrak{p}, \mathfrak{p}^j$ are unramified in Ω_n/\mathbb{L} , so τ restricts to an Artin symbol in this extension. The previous identity implies

$$\left(\frac{\Omega/\mathbb{L}}{a}\right) = \left(\frac{\Omega/\mathbb{L}}{\mathfrak{p}^{j-1}}\right);$$

Since the Artin symbol is a class symbol, we conclude that the primes in the coherent sequence of classes $b = [\mathfrak{p}^{j-1}] \in \mathbf{B}^-$ generate $\text{Gal}(\Omega/\Omega^{\varphi(a)})$ and $a = b$, which completes the proof. \square

4.5. Proof of Theorems 3 and 1. We can turn the discussion of the example above into a proof of Theorem 3 with its consequence, the Corollary 1. The proof generalizes the one given above for imaginary quadratic extensions, by using the construction of the extensions \mathbb{U}_\wp defined above.

Proof. Let $\mathbb{L} = \mathbb{H}_1 \cdot \mathbb{K}_\infty$, like in the previous proof. Let $\wp \subset \mathbb{K}$ be a prime above p and \mathbb{U} be the maximal unramified extension of \mathbb{L} contained in \mathbb{U}_\wp , the extension defined in Lemma 26, and let \tilde{j} be a lift of complex conjugation to $\text{Gal}(\mathbb{U}/\mathbb{Q})$. Since Ω/\mathbb{H}_1 is abelian, the extension \mathbb{U}/\mathbb{H}_1 is also galois and abelian.

Let $\mathfrak{P} \subset \mathbb{U}$ be a fixed prime above \wp and $\tilde{j} \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ be a lift of complex conjugation. Consider the inertia groups $I(\mathfrak{P}), I(\mathfrak{P}^j) \subset \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ be the inertia groups of the two conjugate primes. Like in the example above, $\text{Gal}(\mathbb{U}/\mathbb{H}_1) \cong \mathbb{Z}_p^2$ and $\mathbb{U}_\mathfrak{P}/\mathbb{K}_\wp$ is a product of at most two \mathbb{Z}_p extensions of \mathbb{Q}_p . It follows that the inertia groups are isomorphic to \mathbb{Z}_p and disinct: otherwise, there commone fixed field in \mathbb{U} would be an uramified \mathbb{Z}_p -extension of \mathbb{H}_1 .

For $\nu \in C \setminus \{1, j\}$, the primes above $\nu\wp$ are totally split in $\mathbb{U}_\wp/\mathbb{K}_\infty$, so a fortiori in \mathbb{U} . Let $\tilde{\tau} \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ generate the inertia group $I(\mathfrak{P})$; then $\tilde{\tau}^j \in \text{Gal}(\mathbb{U}/\mathbb{H}_1)$ is a generator of $I(\mathfrak{P}^j)$. Since \mathbb{U}/\mathbb{L} is an unramified extension, there is an $a \in \mathbf{A}^-$ such that

$$\tilde{\tau}^j = j\tilde{\tau}j = \left(\frac{\mathbb{U}/\mathbb{L}}{a}\right) \cdot \tilde{\tau}.$$

Thus

$$(32) \quad \varphi(a) = j\tilde{\tau}j\tilde{\tau}^{-1}.$$

Like in the previous proof, we let $\mathfrak{p} = \mathfrak{P} \cap \mathbb{L}$ and note that since \mathfrak{p} does not ramify in \mathbb{U}/\mathbb{L} , the automorphism $\tilde{\tau}$ acts like the Artin symbol $\left(\frac{\mathbb{U}/\mathbb{L}}{\mathfrak{p}}\right)$. The relation (32) implies:

$$\left(\frac{\mathbb{U}/\mathbb{L}}{a}\right) = \left(\frac{\mathbb{U}/\mathbb{L}}{\mathfrak{p}^{j-1}}\right).$$

In particular, the primes in the coherent sequence of classes $b = [\mathfrak{p}^{j-1}] \in \mathbf{B}^-$ generate $\text{Gal}(\mathbb{U}/\mathbb{L})$ and \mathbb{U} does not split all the primes above p . This happens for all \wp and by Lemma 26 we have $\mathbb{H}_B^- = \prod_{\nu \in C/\{1, j\}} U_{\nu \wp}$, so it is spanned by \mathbb{Z}_p -extensions that do not split the primes above p and consequently

$$[\mathbb{H}'_\infty \cap \mathbb{H}_B] < \infty.$$

We may now apply Lemma 25 which implies that $\mathbf{A}^-(T) = \mathbf{B}^-$. This completes the proof of Theorem 3. The corollary 1 is a direct consequence: since $\mathbf{A}^-(T) = \mathbf{A}^-[T] = \mathbf{B}^-$, it follows directly from the definitions that $(\mathbf{A}')^-(T) = \{1\}$. \square

Remark 5. *The above proof is intimately related to the case when \mathbb{K} is CM and \mathbb{K}_∞ is the \mathbb{Z}_p -cyclotomic extension of \mathbb{K} . The methods cannot be extended without additional ingredients to non CM fields, and certainly not other \mathbb{Z}_p -extensions than the cyclotomic. In fact, Carroll and Kisilevsky have given in [3] examples of \mathbb{Z}_p -extensions in which $\mathbf{A}'(T) \neq \{1\}$.*

A useful consequence of the Theorem 3 is the fact that the \mathbb{Z}_p -torsion of X/TX is finite. As a consequence, if $M = \mathbf{A}[p^\mu]$, $\mu = \mu(\mathbb{K})$, then $Y_1 \cap M^- \subset TX$. In particular, if $a \in M^-$ has $a_1 = 1$, then $a \in TM^-$. We shall give in a separate paper a proof of $\mu = 0$ for CM extensions, which is based upon this remark. Note that the finite torsion of X/TX is responsible for phenomena such as the one presented in the example 5. above.

5. CONCLUSIONS

Iwasawa's Theorem 6 reveals distinctive properties of the main module \mathbf{A} of Iwasawa Theory, and these are properties that are not shared by general Noetherian Λ -torsion modules, although these are sometimes also called "Iwasawa modules". In this paper we have investigated some consequences of this theorem in two directions. The first was motivated by previous results of Fukuda: it is to be expected that the growth of specific cyclic Λ -submodules which preserve the overall properties of \mathbf{A} in Iwasawa's Theorem, at a cyclic scale, will be constrained by some

obstructions. Our analysis has revealed some interesting phenomena, such as

1. The growth in rank of the modules \mathcal{A}_n stops as soon as this rank is not maximal (i.e., in our case, p^{n-1} for some n).
2. The growth in the exponent can occur at most twice before rank stabilization.
3. The most *generous* rank increase is possible for regular flat module, when all the group \mathcal{A}_n have a fixed exponent and subexponent, until rank stabilization, and the exponent is already determined by \mathcal{A}_n . It is an interesting fact that we did not encounter any example of such modules in the lists of Ernvall and Metsänkylä.

Although these obstruction are quite strong, there is no direct upper bound either on ranks or on exponents that could be derived from these analysis.

Turning to infinite modules, we have analyzed in Chapter 4 the structure of the complement of TX in Iwasawa's module Y_1^- in the case of CM extensions. This was revealed to be \mathbf{B}^- , a fact which confirms the conjecture of Gross-Kuz'min in this case.

The methods introduced here suggest the interest in pursuing the investigation of consequences of Iwasawa's Theorem. Interesting open topics are the occurrence of floating elements and their relation to the splitting in the sequence (21) and possible intersections of Λ -maximal modules. It is conceivable that a better understanding of these facts may allow to extend our methods to the study of arbitrary Λ -cyclic submodules of \mathbf{A} . It will probably be also a matter of taste, to estimate whether the detail of the work that such generalizations may require can be expected to be compensated by sufficiently simple and structured final results.

Acknowledgment: The material of this paper grew, was simplified and matured over a long period of time, first as a central target, then as a byproduct of deeper investigations in Iwasawa's theory. I thank all my colleagues at the Mathematical Institute of the University of Göttingen for their support in this time. I thank Victor Vuletescu who actively helped the development of the ideas during the time of the Volkswagen Foundation grant and Tobias Bembom and Gabriele Ranieri for their critical reading and active help with the completion of this paper.

Last but not least, the questions discussed here were the first building block of a series of Seminar lectures held together with S. J. Patterson in the years 2007-08, the notes of which will appear in the sequel in the

series entitled SNOQIT: *Seminar Notes on Open Questions in Iwasawa Theory*. I thank Paddy for the inspirational discussions we had since that time.

REFERENCES

- [1] T. Albu. *Cogalois theory*. Number 252 in Monographs and textbooks in pure and applied mathematics. Marcel Dekker Inc., 2003.
- [2] M. Bhargava. The density of discriminants of quadratic rings and fields. *Ann. Math.*, 162:1031–1063, 2005.
- [3] J. Carroll and H. Kisilevsky. On the iwasawa invariants of certain \mathbb{Z}_p -extensions. *Compositio Mathematica*, 49(2):217–229, 1983.
- [4] H. Cohen and H. W. L. Jr. Heuristics on class groups of number fields. In Springer, editor, *Number Theory, Noordwijkerhout*, volume 1068 of *Lecture Notes in Math.*, pages 33–62, 1984.
- [5] H. Cohen and J. Martinet. étude heuristique des groupes de classes des corps de nombres. *J. reine und angew. Math.*, 404:39–76, 1990.
- [6] R. Ernvall and T. Metsänkylä. Computation of the Zeros of p -Adic L -Functions. *Math. Comp.*, 58(198):815–830, 1992.
- [7] L. Federer and B. Gross. Regulators and Iwasawa modules. *Invent. Math.*, 62(3):443–457, 1981.
- [8] T. Fukuda. Remarks on \mathbb{Z}_p -extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8):264–266, 1994.
- [9] R. Greenberg. On a certain ℓ -adic representation. *Invent. Math.*, 21:117–124, 1973.
- [10] R. Greenberg. On the Iwasawa invariants of totally real fields. *American Journal of Mathematics*, 98:263–284, 1973.
- [11] K. Iwasawa. On \mathbb{Z}_ℓ - extensions of number fields. *Ann. Math. Second Series*, 98:247 – 326, 1973.
- [12] L. Kuz'min. The Tate module for algebraic number fields. *Math. USSR Izvestija*, 6(2):263–321, 1972.
- [13] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined Second Edition edition, 1990.
- [14] S. Lang. *Algebra*. Addison Wesley, second Edition edition, 1994.
- [15] F. Thaine. On the ideal class groups of real abelian number fields. *Ann. of Math. Series 2*, 128(1):1–18, 1988.
- [16] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1996.

(P. Mihăilescu) MATHEMATISCHES INSTITUT DER UNIVERSITÄT GÖTTINGEN
E-mail address, P. Mihăilescu: `preda@uni-math.gwdg.de`